Secure Controls Framework Conformity Assessment Program (SCF CAP)

Cybersecurity Maturity Model Certification (CMMC) Level 1 Third-Party Assessment, Attestation & Certification (3PAAC) Guide & Standards

version 1.0

This publication is available free of charge from: **https://securecontrolsframework.com/content/cap/ag-cmmc-l1.pdf**

Table of Contents

INTRODUCTION

Cybersecurity Maturity Model Certification (CMMC) is a requirement by the US Department of War (DoW) for organizations that store, process and/or transmit:

- Federal Contract Information (FCI); and/or
- Controlled Unclassified Information (CUI).

The CMMC Level 1 Third-Party Assessment, Attestation & Certification (3PAAC) guide and standards is focused on CMMC Level 1 that is narrowly-focused on the protection of FCI. This does not address CMMC Levels 2 or 3.

This document is based on:

- Work by the US DoW specific to the:
  - CMMC Scoping Guide - Level 1 (version 2.13, September 2024);[1]
  - CMMC Assessment Guide – Level 1 (version 2.13, September 2024);[2]
- Work by the Secure Controls Framework Council (SCF Council) specific to the:
  - Secure Controls Framework (SCF);[3]
  - Secure Controls Framework Conformity Assessment Program Body of Knowledge (SCF CAP BoK); [4] and
  - Security & Data Privacy Assessment Standards (CDPAS). [5]

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) LEVEL 1 SELF ATTESTATION OVERVIEW

Organizations subject to CMMC Level 1 can choose from two options:

(1) Perform the annual self-assessment internally; or
(2) Engage a third party to assist.

Use of a third party to assist is still considered a self-assessment and does not result in a certification from the DoW. The primary result of a self-assessment is the submission of Level 1 compliance results into the Supplier Performance Risk System (SPRS) and a self-assessment report, which contains the findings associated with the self-assessment.

FEDERAL CONTRACT INFORMATION (FCI) OVERVIEW

CMMC Level 1 focuses on the protection of FCI, which is defined in 32 CFR § 170.4[6] and 48 CFR § 4.1901[7]:

> *Federal Contract Information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.*

CMMC Level 1 is comprised of the fifteen (15) basic safeguarding requirements specified in Federal Acquisition Regulation (FAR) Clause 52.204-21:[8]

(1) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(2) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(3) Verify and control/limit connections to and use of external information systems.

---

[1] *CMMC Level 1 Scoping Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1v2.pdf*
[2] *CMMC Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf*
[3] *SCF – https://securecontrolsframework.com*
[4] *SCF CAP Body of Knowledge – https://securecontrolsframework.com/content/cap/scf-cap-bok.pdf*
[5] *SCF CDPAS – https://securecontrolsframework.com/content/cdpas.pdf*
[6] *Federal Contract Information (FCI) - https://www.ecfr.gov/current/title-32/part-170/section-170.4#p-170.4(b)(Federal%20Contract%20Information%20(FCI))*
[7] *Federal Contract Information (FCI) - https://www.ecfr.gov/current/title-48/part-4/section-4.1901#p-4.1901(Federal%20contract%20information)*
[8] *FAR 52.204-21 - https://www.acquisition.gov/far/52.204-21*

(4) Control information posted or processed on publicly accessible information systems.
(5) Identify information system users, processes acting on behalf of users, or devices.
(6) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(7) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
(8) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(9) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(10) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(11) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(12) Identify, report, and correct information and information system flaws in a timely manner.
(13) Provide protection from malicious code at appropriate locations within organizational information systems.
(14) Update malicious code protection mechanisms when new releases are available.
(15) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

SCF Conformity Assessment Program (SCF CAP) Overview

The goal of the Secure Controls Framework (SCF) is to provide a powerful tool and methodology that will advance how cybersecurity & data protection controls are implemented and assessed at an organization's strategic, operational and tactical layers, regardless of its size or industry.

The SCF Council established the Secure Controls Framework Conformity Assessment Program (SCF CAP) as a structure to conduct cybersecurity and data protection-related Third-Party Assessment, Attestation and Certification Services (SCF 3PAAC Services).[9] There is a need for a scalable, cost-effective solution to obtain a company-level, third-party assessment of cybersecurity & data protection practices and the SCF CAP addresses that need.

The SCF CAP exists to leverage SCF content to provide a company-level certification through a conformity assessment process. The SCF CAP is designed to make conformity assessments more cost-effective, efficient and objective through the use of the SCF's metaframework structure and no-cost content.

As a metaframework, the SCF CAP allows for a singular certification approach to cybersecurity & data protection requirements where it:

- Utilizes an examine, interview and test assessment methodology to demonstrate conformity with multiple requirements. This approach allows the SCF CAP to scale to cover multiple requirements simultaneously (e.g., demonstrate conformity with NIST CSF, HIPAA, EU GDPR, etc.) as part of a single assessment;
- Allows an organization to specify the statutory, regulatory and contractual obligations that are applicable to establish a Minimum Security Requirements (MSR) control set; and
- Leverages leading industry assessment practices to avoid "re-inventing the wheel" for assessment methodologies.

The SCF CAP:

- Is designed to produce a deliverable Report on Conformity (ROC) with a designation that summarizes the organization's overall cybersecurity & data protection program.
- Leverages concepts established in the CDPAS. [10]
- Can be scaled to provide conformity assessments for:
  - An entire organization;
  - A specific contract, project or initiative;
  - A specific Business Unit (BU) within an organization; or
  - A specific country, or geographic region, of the organization's business operations.

[9] *SCF CAP - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*
[10] *Cybersecurity & Data Privacy Assessment Standards (CDPAS) - https://securecontrolsframework.com/content/cdpas.pdf*

The SCF CAP BoK provides details on the SCF Certification process, including criteria necessary to obtain an SCF Certified™ certification.

Third-Party Assessment, Attestation and Certification (3PAAC)

Third-Party Assessment, Attestation and Certification (3PAAC) addresses:

- Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization.[11]
- Attestation: The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated.[12]
- Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.[13]

As part of SCF 3PAAC Services, a Third-Party Assessment Organization (SCF 3PAO) is expected to perform the following three (3) fundamental 3PAAC functions:

(1) Conduct a conformity assessment of applicable cybersecurity and/or data protection controls within the OSA's assessment boundary;
(2) Provide an attestation based on the findings from the conformity assessment in a Report on Conformity (ROC); and
(3) Authorize the issue of a **SCF Certified™ - CMMC Level 1** certification, if sufficient conformity is achieved.

This document provides CMMC Level 1-specific conformity assessment guidance for conducting SCF 3PAAC Services, as part of the SCF CAP. An organization must achieve an assessment determination statement level of (1) Conforms or (2) Strictly Conforms to achieve status as **SCF Certified™ - CMMC Level 1**.

Normative References

The following normative references contain material that must be understood and used to utilize SCF 3PAAC Services to achieve status as **SCF Certified™ - CMMC Level 1**:

(1) CMMC Scoping Guide - Level 1 (version 2.13, September 2024);[14]
(2) CMMC Assessment Guide – Level 1 (version 2.13, September 2024);[15]
(3) NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings*;[16]
(4) Set Theory Relationship Mapping (STRM) – CMMC Level 1;[17]
(5) Cybersecurity & Data Protection Assessment Standards (CDPAS);[18] and
(6) SCF Conformity Assessment Program Body of Knowledge (SCF CAP BoK).[19]

Intended Audience

The intended audience of this assessment guide is those parties that encompass the "assessment ecosystem," which includes:

- OSA;
- Third-Party Assessment Organizations (SCF 3PAOs);
- SCF Assessors; and
- External Service Providers (ESP):

[11] *NIST Glossary for Assessment - https://csrc.nist.gov/glossary/term/assessment*
[12] *NIST Glossary for Attestation - https://csrc.nist.gov/glossary/term/attestation*
[13] *NIST Glossary for Certification - https://csrc.nist.gov/glossary/term/certification*
[14] *CMMC Level 1 Scoping Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1v2.pdf*
[15] *CMMC Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf*
[16] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*
[17] *SCF STRM for CMMC 2.0 Level 1 - https://securecontrolsframework.com/content/strm/scf-strm-us-fed-dod-cmmc-2-level-1.pdf*
[18] *CDPAS download - https://securecontrolsframework.com/content/cdpas.pdf*
[19] *SCF CAP BoK download - https://content.securecontrolsframework.com/scf-cap-bok.pdf*

- Consultants;
- Cloud Service Providers (CSP);
- Managed Service Providers (MSP); and
- Managed Security Services Providers (MSSP).

The successful use of this document is predicated on an assumption that the reader has a baseline understanding of the:

- SCF's content; and
- SCF CAP's processes.

Assessment Scoping

CMMC Level 1 scoping guidance provides authoritative guidance on in-scope versus out-of-scope assets, where:[20]

- In-Scope Assets are defined in 32 CFR § 170.19(b)(1) as "information systems which process, store, or transmit FCI."[21]
- Out-of-Scope Assets are defined in 32 CFR § 170.19(b)(2)(i) as "information systems which do not process, store, or transmit FCI are outside the scope for CMMC Level 1." [22]

Per 32 CFR § 170.19(b)(2)(ii), Specialized Assets are not part of the Level 1 CMMC Assessment Scope and are not assessed against CMMC security requirements. [23] Specialized Assets include assets that can process, store, or transmit FCI but are unable to be fully secured, including:

- Internet of Things (IoT) devices;
- Industrial Internet of Things (IIoT) devices;
- Operational Technology (OT);
- Government Furnished Equipment (GFE); and
- Restricted Information Systems, and Test Equipment.

Scoping Due Diligence

Prior to engaging a SCF 3PAO for SCF 3PAAC Services, the OSA must specify the assessment scope. The assessment boundary demarcation can be defined as one (1) of the following four (4) scoping options:

(1) Organization-wide;
(2) A specific contract, project or initiative;
(3) A specific Business Unit (BU) within the OSA; or
(4) A specific country, or geographic region, of the organization's business operations.

To define the demarcation of the assessment boundary:

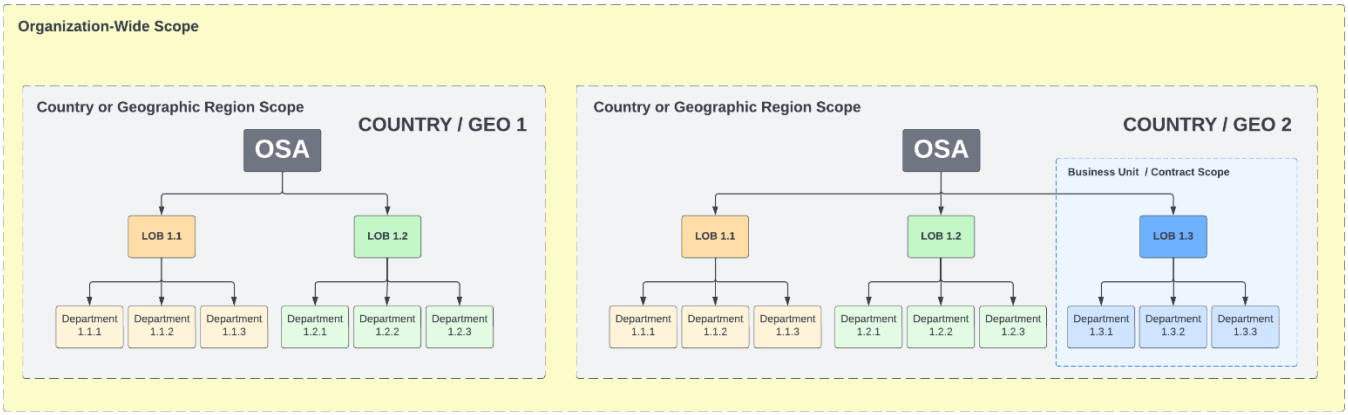
- For an organization-wide scope, it is defined by a discrete:
  - Taxpayer Identification Number (TIN);
  - Employer Identification Number (EIN);
  - Value Added Tax (VAT);
  - Dun & Bradstreet Data Universal Numbering System (DUNS); or
  - If applicable, a Commercial And Government Entity (CAGE) Code.
- For a contract, project, product or initiative, it is defined by:
  - Sufficient detail to describe the scope of the assessment boundary:
    - People;
    - Processes;
    - Technologies;
    - Data; and
    - Facilities;
  - Contract number and/or the name of the project or initiative; and
  - If applicable, a CAGE Code that is associated with the contract.
- For a BU, country or geographic region, it is defined by:
  - Sufficient detail to describe the scope of the assessment boundary:

[20] *CMMC Level 1 Scoping Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1v2.pdf*
[21] *32 CFR § 170.19(b)(1) - https://www.ecfr.gov/current/title-32/part-170/section-170.19#p-170.19(b)(1)*
[22] *32 CFR § 170.19(b)(2(i)) - https://www.ecfr.gov/current/title-32/part-170/section-170.19#p-170.19(b)(2)(i)*
[23] *32 CFR § 170.19(b)(2(ii)) - https://www.ecfr.gov/current/title-32/part-170/section-170.19#p-170.19(b)(2)(ii)*

- People;
- Processes;
- Technologies;
- Data; and
- Facilities;

- OSA-designated name for the BU, country(ies) or geographic region; and
- If applicable, a CAGE Code that is associated with the BU.

A graphical representation of this assessment scoping is shown below:



For CMMC Level 1 purposes, the DoD's CMMC Scoping Guide – Level 1 is the authoritative guidance for determining scope.[24] However, the SFC Council recognizes the Unified Scoping Guide (USG) as an additional guide to determine scope.[25]

Updates

Updates to the SCF CAP will be communicated via an advisory:

- Email notification (e-mail) to active SCF ecosystem stakeholders, including but not limited to:
  - SCF 3PAOs; and
  - SCF Assessors; and
- Blog posting on the SCF website for all others.

Errata will be provided to indicate:

- New content;
- Edited content; and/or
- Deleted/deprecated content.

When a new version of the SCF CAP or 3PAAC Guide & Standards is published, the previous version(s) is deprecated one hundred eighty (180) days after the release of the new version.

Additional SCF CAP-related guidance may be published to the SCF website (e.g., Frequently Asked Questions (FAQ)) without an advisory email notification or blog posting.

Liability Limitations

THIS CONTENT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE CONTENT OR THE USE OR OTHER DEALINGS IN THE CONTENT.

[24] *CMMC Scoping Guide – Level 1 - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1v2.pdf*
[25] *Unified Scoping Guide USG) - https://unified-scoping-guide.com*

TERMINOLOGY & ACRONYMS

The SCF Council recognizes two (2) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[26] and
- NIST Glossary.[27]

TERMINOLOGY STANDARDIZATION

From the context of applying a standard to SCF 3PAAC Services, it is important to clarify mandatory versus optional criteria:[28]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

Note: For CMMC Level 1-speific terms, refer to the CMMC Assessment Guide – Level 1 (version 2.13, September 2024) [29]

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Assurance. Grounds for justified confidence that a security or privacy claim has been or will be achieved. [30]
- Compensating Control. Alternative cybersecurity and/or data protection controls implemented in lieu of the deficient control that provide equivalent or comparable protection. Compensating controls:
  - Include physical, administrative and/or technical safeguards or countermeasures employed by an organization in lieu of the deficient control; and
  - Reduce risk to the affected system(s), service(s), application(s), service(s), individual(s) and/or organization(s) in a manner that is equivalent to, or comparable to, the protection offered if the deficient control was operational and effective.
- Conformity Assessment. A demonstration that specified requirements are fulfilled. To learn more about conformity assessments, NIST published Special Publication 2000-01, *ABC's of Conformity Assessment*, that serves as a worthwhile primer on the subject.[31]
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed,

[26] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[27] *NIST Glossary - https://csrc.nist.gov/glossary*
[28] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*
[29] *CMMC Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf*
[30] *NIST Glossary for Assurance - https://csrc.nist.gov/glossary/term/assurance*
[31] *NIST SP 2000-1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-01.pdf*

authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [32]

- Implemented Capability. An implemented capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.
- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data privacy control that:
  - It is not capable of having compensating controls; and
  - Its absence, or failure, exposes an organization to such a degree that it could have a material impact.
- Material Risk. When an identified risk that poses a material impact, that is a material risk.
  - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
  - A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
  - A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
  - A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
  - A material incident is an occurrence that does or has the potential to:
    - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
    - Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
  - Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.
  - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, etc.).
  - A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.
- Mechanism. A mechanism can be described as a: [33]
  - Process or system that is used to produce a particular result; or
  - Device or method for achieving a security-relevant purpose.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [34]
  - Security assessments to reuse system resources; and/or
  - Assessed security posture to share information.
- Risk. A risk is:
  - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
  - To expose someone or something valued to danger, harm or loss (verb).

[32] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*
[33] *NIST Glossary for Mechanism - https://csrc.nist.gov/glossary/term/mechanism*
[34] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*

- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.[35]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.[36]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[37]
- Security. A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.[38]
- Threat. A threat:
  - Is a person, or thing, likely to cause damage or danger (noun); or
  - Indicates impending damage or danger (verb).
- Trust. A belief that an entity meets certain expectations and therefore, can be relied upon.[39]

ACRONYMS

The following acronyms are used throughout the assessment guide:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations.
3PA	Third-Party Attestation	3PA are attestations made by a third-party, generally in the performance of an assessment or audit.
3PAAC	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party organization.
SCF 3PAO	Third-Party Assessment Organization	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AO	Assessment Objective	AOs are objective statements that establish the purpose and intended outcome of the assessment for a specific control. There may be multiple AOs associated with a control.
APIT	Automated Point In Time	APIT assessments utilize automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence: ▪ Relevant to a specific point in time (time at which the control was evaluated); ▪ In situations where technology cannot evaluate evidence, evidence is manually reviewed; and ▪ The combined output of automated and manual reviews of artifacts is used to derive a finding.
ATE	Assessment Technical Expert	ATE are assessment team members who have the necessary subject matters expertise to conduct a specific part of an assessment. ATE report to the ATL.
ATL	Assessment Team Lead	An ATL is an individual assigned by the SCF 3PAO to lead the assessment team in the conduct of SCF 3PAAC Services.
AEHR	Automated Evidence with Human Assessment	AEHR assessments are used for ongoing, continuous control assessments: ▪ AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and ▪ Recurring human reviews:

[35] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[36] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[37] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*
[38] *NIST Glossary for Security - https://csrc.nist.gov/glossary/term/security*
[39] *NIST Glossary for Trust - https://csrc.nist.gov/glossary/term/trust*

		○ Evaluate the legitimacy of the results from automated control assessments; and ○ Validate the automated evidence review process to derive a finding.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data privacy controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the SCF 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services; ▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
IC	Implemented Capability	IC refer to technical, administrative and physical controls where: ▪ Technology capabilities will only be considered implemented if the system(s), application(s) and/or service(s) has/have been operational in a production environment for at least sixty (60) days; ▪ Administrative processes will only be considered implemented if there is evidence to demonstrate that process has been: ○ Used in a real-world situation (e.g., onboarding/offboarding personnel, incident response, etc.); and/or ○ Formally tested (e.g., documented incident response exercise); and ▪ Physical capabilities will only be considered implemented if the physical security mechanism(s) has/have been operational in a production environment for at least thirty (30) days.
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MPIT	Manual Point In Time	MPIT is a traditional assessment methodology that: ▪ Is relevant to a specific point in time (time at which the control was evaluated); and ▪ Relies on the manual review of artifacts to derive a finding.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OSA	Organization(s) Seeking Assessment	A company, entity or business unit seeking the external assessment.
PbD	Privacy by Design	Data privacy through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator);

		▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment determination statement. The ROC summarizes the assessment findings.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

SCF CAP Assessment Criteria Overview

The SCF CAP is designed to be objective and assess an organization based on the merits of its cybersecurity and data protection program. The SCF CAP uses standardized terminology to clearly indicate status:

- At the control-level, the SCF CAP assigns a control designation; and
- At the assessment boundary-level, the SCF CAP assigns an assessment conformity designation (e.g., certification).

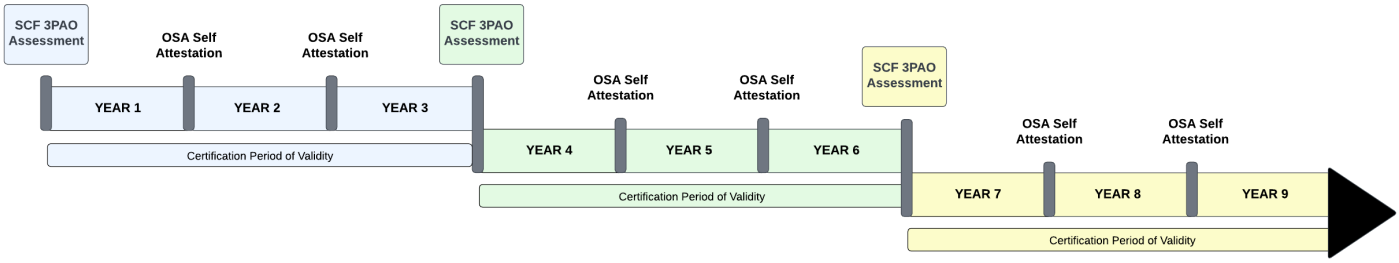
SCF CAP Certification Lifecycle

Throughout the lifecycle of the **SCF Certified™ - CMMC Level 1** certification, it is the responsibility of the OSA to ensure applicable controls are implemented and governed to maintain conformity.

The lifecycle of a **SCF Certified™ - CMMC Level 1** certification is three (3) years:

- During the first year (Year 1) of being certified:
  - The date of the Report on Conformity (ROC) indicates the starting date of the OSA's certification lifecycle.
  - The OSA is required to perform ongoing due care activities to maintain conformity (e.g., ongoing maintenance, change management, managing compliance requirements, etc.).
- During the second year (Year 2) of being certified:
  - The OSA is required to perform ongoing due care activities to maintain conformity.
  - No later than the first anniversary of the date of the ROC, the OSA it required to perform an internal assessment and provide a self-attestation that the OSA continues to conform with applicable controls.
- During the third year (Year 3) of being certified:
  - The OSA is required to perform ongoing due care activities to maintain conformity.
  - No later than the second anniversary of the date of the ROC, the OSA it required to perform an internal assessment and provide a self-attestation that the OSA continues to conform with applicable controls.
- At the end of the third year (Year 3) of being certified:
  - Original **SCF Certified™ - CMMC Level 1** certification expires.
  - A new third-party assessment by a SCF 3PAO is required to issue a new **SCF Certified™ - CMMC Level 1** certification.

This multi-year lifecycle process can be visualized below:



SCF CAP Control Designations

At the control-level, SCF Assessors must designate a status to assessed controls as follows:

(1) There are four (4) possible designations:
   a. Satisfactory;
   b. Deficient;
   c. Compensating Control; or
   d. Not Applicable (N/A); and

(2) For a SCF control to be designated as Satisfactory, each of the control's applicable AOs must be designated as:
   a. Satisfactory;
   b. Compensating Control; or
   c. N/A; and

(3) If all of the following conditions exist, a SCF control designated as Deficient may be re-evaluated during the course of the assessment and for up to ten (10) business days following the active assessment period:
   a. Additional evidence:

i. Is available to demonstrate the control is satisfied; and
ii. Cannot change, or limit the effectiveness of, other requirements that have previously been scored Satisfactory; and

b. The Report on Conformity (ROC) has not been delivered to the OSA.

In the context of control designations, a designation of:

SATISFACTORY

Satisfactory is positive, where all applicable AOs are designated as:

- Satisfied;
- N/A; or
- An compensating control is validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

DEFICIENT

Deficient is negative, where one (1), or more, applicable AOs are designated as:

- Deficient; or
- An compensating control cannot be validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

COMPENSATING CONTROL

Compensating Control is neutral, where:

- Another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and
- The compensating control(s) is/are validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

NOT APPLICABLE (N/A)

N/A is neutral, where the control, or AO, does not apply.

SCF CAP ASSESSMENT CONFORMITY DESIGNATION

At the assessment boundary-level, SCF 3PAOs will produce a written Report on Conformity (ROC) that leverages reasonable evidence to defend the assessment conformity designation. Only one (1) of the following four (4) possible conformity designations may be used:

(1) Strictly Conforms;
(2) Conforms;
(3) Significant Deficiency; or
(4) Material Weakness.

From a pass/fail perspective, conformity designations can be viewed as:

- Passing conformity designations include:
  - Strictly Conforms; and
  - Conforms.
- Failing conformity designations include:
  - Significant Deficiency; and
  - Material Weakness.

STRICTLY CONFORMS

The designation of Strictly Conforms is a **positive outcome** and indicates the OSA can demonstrate Strict Conformity with its selected cybersecurity and/or data privacy controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:

(1) The controls are met and operational;
(2) Any control designated as Not Applicable (N/A) is validated as such by the SCF Assessor; and/or
(3) Where applicable, compensating controls are validated by the SCF Assessor as being:
    a. Applicable;
    b. Reasonable; and
    c. Implemented and operating properly; and
(4) Assessed controls provide reasonable assurance that the OSA's cybersecurity and data privacy program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks;
    c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
    d. Is prepared to respond to material incidents.

CONFORMS

The designation of Conforms is a **positive outcome** and indicates the OSA can demonstrate conformity with its selected cybersecurity and/or data privacy controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:

(1) The controls are met and operational;
(2) Any control designated as N/A is validated as such by the SCF Assessor; and/or
(3) Where applicable, compensating controls are validated by the SCF Assessor as being:
    a. Applicable;
    b. Reasonable; and
    c. Implemented and operating properly;
(4) Any assessed control deficiency is not material to the OSA's cybersecurity and data privacy program; and
(5) Assessed controls provide reasonable assurance that the OSA's cybersecurity and data privacy program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks;
    c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
    d. Is prepared to respond to material incidents.

SIGNIFICANT DEFICIENCY

The designation of Significant Deficiency is a **negative outcome** and indicates the OSA can demonstrate limited conformity with its selected cybersecurity and/or data privacy controls due to a systemic problem within the OSA's cybersecurity and data privacy program, where:

(1) At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
    a. The controls are met and operational;
    b. Any control designated as N/A is validated as such by the SCF Assessor; and/or
    c. Where applicable, compensating controls are validated by the SCF Assessor as being:
        i. Applicable;
        ii. Reasonable; and
        iii. Implemented and operating properly;
(2) Any assessed control deficiency is not material to the OSA's cybersecurity and data privacy program;
(3) Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data privacy program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks;
    c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
    d. Is prepared to respond to material incidents; and
(4) The OSA's cybersecurity and data privacy program:

a. Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
b. Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data privacy controls.

Material Weakness

The designation of Material Weakness is a **negative outcome** and indicates where the OSA cannot demonstrate conformity with its selected cybersecurity and/or data privacy controls due to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:

(1) One (1), or more, material controls is/are deficient;
(2) Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
    a. The controls are met and operational;
    b. Any control designated as N/A is validated by the SCF Assessor and confirmed as such; and/or
    c. Where applicable, compensating controls are validated by the SCF Assessor as being:
        i. Applicable;
        ii. Reasonable; and
        iii. Implemented and operating properly;
(3) Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data privacy program adequately:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks; and/or
    c. Possesses the capability to:
        i. Detect and protect against material cybersecurity and/or data privacy threats; and/or
        ii. Respond to material incidents; and
(4) The OSA's cybersecurity and data privacy program:
    a. Cannot perform its stated mission; and
    b. Necessitates drastic changes to people, processes and/or technologies to remediate the deficiencies.

SCF CAP Assessment Methods

SCF 3PAOs must use the assessment methods and criteria as defined in this section to conduct a **SCF Certified™ - CMMC Level 1** conformity assessment. SCF Assessors will review artifacts and other evidence to independently verify that an OSA meets the Assessment Objectives (AOs) for all applicable controls.

From an assessment perspective, the SCF provides numerous components to assist in an assessment:

- An Evidence Request List (ERL) that identifies appropriate, control-specific artifacts for SCF Assessors to examine;
- AOs to define criteria that must be met to reasonably satisfy a control objective; and
- A Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) that contains Maturity Level Criteria (MLC) to identify possible processes and/or technologies to test.

SCF Assessors must perform the assessment according to the assessment method specified in the Statement of Work (SOW). SCF 3PAO must specify one (1) of the three (3) following assessment rigors:

The SCF 3PAO must specify one (1) of the three (3) following assessment methods:

(1) Manual Point In Time (MPIT);
(2) Automated Point In Time (APIT); or
(3) Automated Evidence with Human Review (AEHR).

Manual Point In Time (MPIT)

MPIT is a traditional assessment methodology that:

- Is relevant to a specific point in time (time at which the controls were evaluated); and
- Relies on the manual review of artifacts to derive a finding.

Automated Point In Time (APIT)

APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

- Is relevant to a specific point in time (time at which the controls were evaluated);
- In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
- The combined output of automated and manual reviews of artifacts is used to derive a finding.

Automated Evidence with Human Review (AEHR)

AEHR is used for ongoing, continuous control assessments:

- AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
- Recurring human reviews:
  - Evaluate the legitimacy of the results from automated control assessments; and
  - Validate the automated evidence review process to derive a finding.

Note: APIT and AEHR may leverage Artificial Intelligence and/or Machine Learning (AI/ML) technologies. In the case of AI/ML being used, SCF 3PAOs must be prepared to demonstrate sufficient evidence of due diligence and due care to justify the integrity of the findings and overall assessment results (e.g., evidence of validating results, test cases, etc.).

SCF CAP Assessment Criteria

At a minimum:

- Standard rigor should be used for MPIT assessments;
- Enhanced rigor should be used for APIT assessments; and
- Comprehensive rigor should be used for AEHR assessments.

SCF Assessors must perform the assessment at a level of rigor specified in the Statement of Work (SOW). SCF 3PAO must specify one (1) of the three (3) following assessment rigors:

1. Level 1: STANDARD;
2. Level 2: ENHANCED; or
3. Level 3: COMPREHENSIVE.

Level 1 Rigor: Standard

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

- Implemented; and
- Free of obvious errors.

Level 2 Rigor: Enhanced

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

- The applicable controls are:
  - Implemented; and
  - Free of obvious/apparent errors; and
- There are increased grounds for confidence that the applicable controls are:
  - Implemented correctly; and
  - Operating as intended.

Level 3 Rigor: Comprehensive

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

- Whether the applicable controls are:
- Implemented; and
- Free of obvious/apparent errors;

- Whether there are further increased grounds for confidence that the applicable controls are:
- Implemented correctly; and
- Operating as intended on an ongoing and consistent basis; and
- There is support for continuous improvement in the effectiveness of the applicable controls.

Note: SCF 3PAO are expected to develop clear criteria for determining the level of rigor (Standard, Enhanced, Comprehensive) based on the OSA's needs, risk appetite and risk profile.

AUTHORITATIVE MAPPINGS FOR PERFORMING CONFORMITY ASSESSMENTS

To perform a conformity assessment, the methodology requires:

- Authoritative mappings;
- Reasonable granularity to address the intent of the control; and
- Objective criteria to determine if the control is adequately:
  - Designed;
  - Implemented; and
  - Operating as intended.

As part of the CMMC Assessment Guide – Level 1, there is authoritative guidance for:[40]

- Scoping guidance;
- Assessment Objectives (AOs);
- Criteria for assessment methods (e.g., examine, interview & test); and
- Additional reference guidance.

Note: For CMMC Level 1-speific Assessment Objectives (AOs), refer to the CMMC Assessment Guide – Level 1 (version 2.13, September 2024).[41] Those AOs are also available in Annex 1 – CMMC L1 Requirements. The SCF CAP leverages the authoritative information provided in the CMMC Assessment Guide – Level 1 to enable an SCF-based conformity assessment to be performed, where:

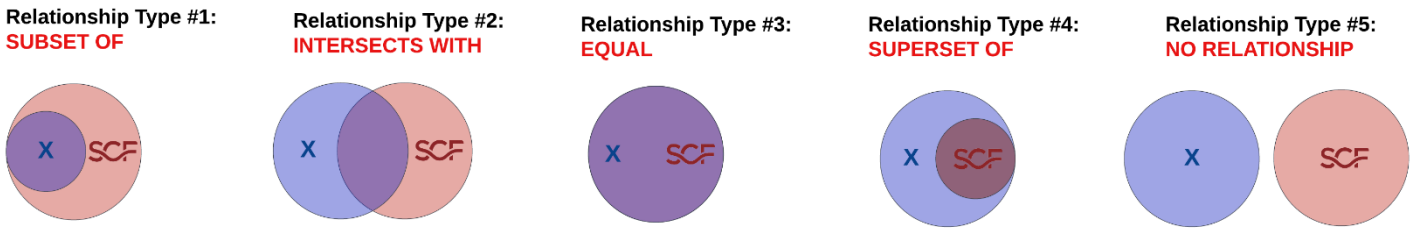
- CMMC Level 1 AOs are used to determine if CMMC Level 1 requirements are met; and
- CMMC Level 1 AOs are mapped to SCF controls using Set Theory Relationship Mapping (STRM).

NIST IR 8477 - BASED SET THEORY RELATIONSHIP MAPPING (STRM)

The SCF leverages NIST IR 8477 STRM guidelines for crosswalk mapping, since STRM is generally well-suited to evaluate cybersecurity and data privacy laws, regulations and frameworks.[42] NIST IR 8477 is the US Government's playbook for how to perform crosswalk mapping between different cybersecurity and data privacy laws, regulations and frameworks.

STRM is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two (2) distinct concepts:

(1) Subset Of;
(2) Intersects With;
(3) Equal;
(4) Superset Of; and
(5) No Relationship.



Specific to STRM terminology:

- **Reference Document** – This will always be the SCF. The Reference Document is being mapped to the Focal Document.
- **Focal Document** – This will always be the law, regulation or framework is the source document that is being mapped from (e.g., CMMC Level 1).

[40] *CMMC Scoping Guide – Level 1 - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf*
[41] *CMMC Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf*
[42] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*

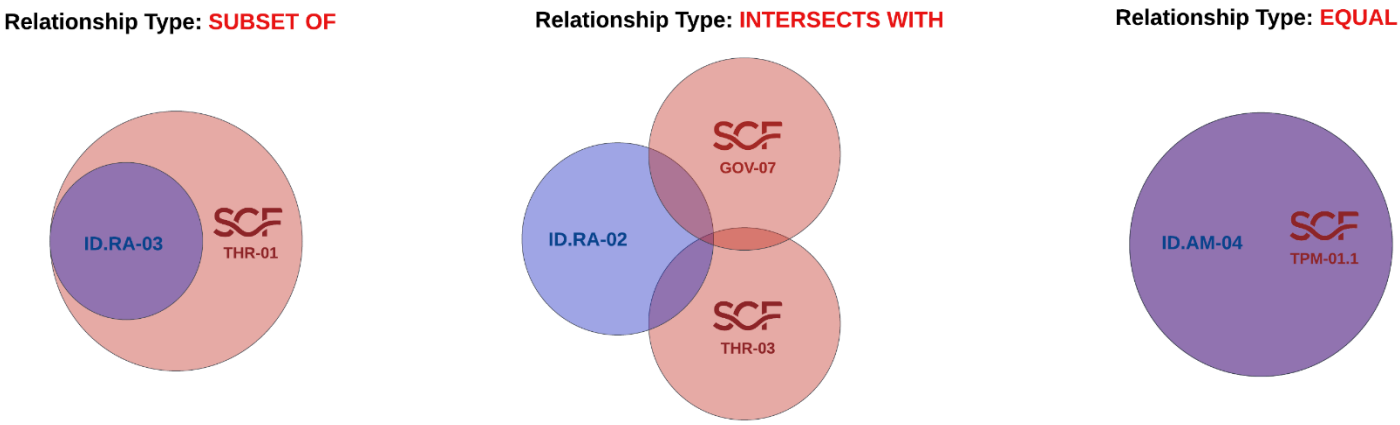
- **Focal Document Element (FDE)** – This is the granular requirement/control from the Focal Document to is being mapped to.

STRM also allows the strength of the mapping to be captured, where STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two (2) concepts are related:

(1) Syntactic: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
(2) Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
(3) Functional: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Note: SCF mappings leverage only Function context justification for STRM.

The use of STRM enables the SCF to create "backwards mapping" from CMMC Level 1 to SCF controls that are justifiable, based on relationship types and the rationale used to perform the mapping. Graphical examples for STRM relationships between NIST CSF 2.0 and SCF are shown below:



These STRM graphics can be downloaded from:
https://securecontrolsframework.com/content/strm/scf-set-theory-relationship-mapping.pdf

APPLICABLE SCF STRM VERSION

The most current version of the SCF should be used for SCF CAP purposes.[43] As the applicable STRM for a law, regulation or framework is released/updated, a new version of the SCF STRM will be generated. When a new version of STRM is published, the previous version is deprecated one hundred eighty (180) days after the release of the new version.

[43] *SCF Download - https://securecontrolsframework.com/scf-download/*

CMMC Level 1: Third-Party Assessment, Attestation and Certification (3PAAC) Standards

The SCF Third-Party Assessment, Attestation and Certification Assessment Guide Standards (SCF 3PAAC AGS) are based on the Cybersecurity & Data Protection Assessment Standards (CDPAS).[44] The CDPAS provides an industry standard, where exceptions by either OSA or SCF 3PAOs must be justified. If additional clarification is required, the CDPAS provides additional context for the standards in the form of justifications and guidelines.

The 3PAAC Standards apply to:

- OSAs;
- SCF Assessors; and
- SCF 3PAOs.

3PAAC Standard 1: Professional Duty of Care

SCF Assessors must exercise due diligence and due care by using their skills and knowledge to reach informed, objective decisions when conducting Third-Party Assessment, Attestation & Certification Services (3PAAC Services).

Justification: Assessors and Third-Party Assessment Organizations (SCF 3PAOs) operate in a position of trust and authority. Therefore, assessors and SCF 3PAOs must exercise due diligence and due care in the conduct of their business interactions and representation of professionalism in business interactions.

Guidance: There is a professional obligation for cybersecurity and/or data privacy practitioners to provide reasonable services and skills to their clients. SCF 3PAOs and assessors are expected to be familiar with the industry norms associated with client 3PAAC Service engagements, due to the specialized knowledge that may be required as part of the assessment.

3PAAC Standard 1.1: Ethical Conduct

SCF Assessors must:

(1) Act ethically, professionally and legally towards clients, employers, colleagues and society; and

(2) Adhere to ethical principles and values in personal and professional endeavors, specifically being honest, forthright and trustworthy.

Justification: Assessors operate from a position of trust and authority. Therefore, assessors are expected to conduct themselves professionally. Unprofessional conduct can harm the SCF 3PAO and the Organization Seeking Assessment (OSA).

Guidance: Organizations providing 3PAAC Services are reasonably expected to have formalized standards of conduct (e.g., rules of behavior) that their employees and contractors are contractually obligated to adhere to. Those documented standards of conduct can help define an assessor's formal role and responsibilities. Violations of those standards of conduct are expected to be addressed through Human Resources (HR)-related enforcement mechanisms that includes personnel sanctions. HR enforcement actions are expected to reflect the severity of the conduct violation.

3PAAC Standard 1.2: Independence

SCF Assessors must maintain objectivity and be free to exercise professional judgment.

Justification: Assessors operate from a position of trust and authority. Therefore, assessors must operate independently and exercise professional judgment without bias or influence. Without assessor independence:

- *The integrity of the assessment should be considered compromised; and*
- *Any final report or related observations should be dismissed as untrustworthy, requiring a re-assessment by a different SCF 3PAO.*

Guidance: Ensuring assessor independence may be achieved through:

- *Avoiding Conflicts of Interest (COI);*
- *Sound hiring practices; and*

[44] *SCF CDPAS - https://securecontrolsframework.com/content/cdpas.pdf*

- *Top-down evaluations to uncover dysfunctional management practices.*

3PAAC Standard 1.3: Subject Matter Competency

SCF Assessors must:

(1) Have documented evidence of relevant job experience and relevant training to demonstrate proficiency in performing assessment duties; and

(2) Annually, complete at least twenty (20) hours of Continuing Professional Education (CPE) training in topics relevant to the skills and situational awareness necessary to be an effective assessor.

Justification: It is reasonable to expect an assessor to be a demonstrable Subject Matter Expert (SME) in cybersecurity and/or data protection practices. Being able to demonstrate this will be through relevant, ongoing skill development:

- *Industry-recognized cybersecurity and/or data privacy certifications;*
- *Industry involvement (e.g., conference panels); and*
- *Other training opportunities (e.g., online or in-person training events).*

Guidance: It is possible to complete the annual CPE requirements concurrently with other professional certifications. While it is impossible to have expertise in every highly technical subcategory of the cybersecurity profession, it is reasonable to expect that an assessment team will bring in Assessment Technical Experts (ATE), with subject matters expertise to conduct their specific part of an assessment, as necessary. SCF 3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on specialized technical assessments, including:[45]

- *Application security testing and examination; and*
- *Remote access testing.*

The US Department of Defense Manual (DODM) 8140.03, Cybersecurity Workforce Qualification and Management Program, contains a listing of industry certifications for various cybersecurity-related positions. [46] *The Security Control Assessor (role ID# 612) from DODM 8140.3 provides an industry standard for minimum certifications that is applicable to:* [47]

- *Entry-level assessor;*
- *Intermediate-level assessor; and*
- *Senior-level assessor.*

In addition to practical, hands-on experience, this DODM guidance should be used by SCF 3PAOs to establish a baseline level of subject matter competency necessary to perform 3PAAC Services:

- *Entry and intermediate-level assessor:*
  - *An undergraduate (Bachelor of Science) degree fulfills the educational requirement if it is:*
    - *From an:*
      - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
      - *Centers of Academic Excellence (CAE) designated institution.*
    - *In the one of the following degrees:*
      - *Information Technology (IT)*
      - *Cybersecurity;*
      - *Data Science;*
      - *Information Systems; or*
      - *Computer Science (CS);*

  and/or

  - *One (1) of the following certifications:*
    - *CGRC/CAP - ISACA Certified in Governance, Risk, and Compliance (formerly known as CAP);*
    - *GSEC - GIAC Security Essentials Certification;*
    - *CASP+ - CompTIA Advanced Security Practitioner plus;*
    - *Cloud+ - CompTIA Cloud plus;*
    - *PenTest+ - CompTIA Penetration Tester plus; and/or*
    - *Security+ - CompTIA Security plus.*

[45] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*
[46] *DoDM 8140.03 - https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*
[47] *DoD 8140 Qualification Matrices - https://public.cyber.mil/wid/dod8140/qualifications-matrices/*

- *Senior-level assessor:*
  - *An undergraduate degree fulfills the educational requirement if it is:*
    - *From an:*
      - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
      - *Centers of Academic Excellence (CAE) designated institution.*
    - *In the one of the following degrees:*
      - *Information Technology (IT)*
      - *Cybersecurity;*
      - *Data Science;*
      - *Information Systems; or*
      - *Computer Science (CS);*

and/or

  - *One (1) of the following certifications:*
    - *CISM - ISACA Certified Information Security Manager;*
    - *CISA - ISACA Certified Information Systems Auditor;*
    - *CISSP - ISC2 Certified Information Systems Security Professional;*
    - *CISSP-ISSEP - ISC2 CISSP - Information Systems Security Engineering Professional;*
    - *GCSA - GIAC Cloud Security Automation;*
    - *GSLC - GIAC Security Leadership Certification;*
    - *GSNA - GIAC Systems and Network Auditor;*
    - *CySA+ - CompTIA Cybersecurity Analyst plus;*
    - *C)ISSO - Certified Information Systems Security Officer;*
    - *C)PTE - Certified Penetration Testing Engineer; and/or*
    - *FITSP-A - Federal IT Security Professional-Auditor.*

3PAAC STANDARD 1.4: CONFLICT OF INTEREST (COI) AVOIDANCE

SCF Assessors must avoid actual and/or perceived COI. COI includes involvement in the design, or implementation, of any of the OSA's cybersecurity and/or data protection controls, which are reasonably expected, or intended, to be included in the scope of the assessment:

(1) An assessor is prohibited from conducting 3PAAC Services if the assessor made a material impact on the OSA's cybersecurity and data protection program; and

(2) Materiality impact is defined as:

a. Material Impact - Within the past five (5) years, the assessor made a significant impact on the OSA's cybersecurity and/or data protection program, where the assessor performed a broad scope of work with a strategic and/or operational impact on the OSA's cybersecurity and/or data protection controls; and

b. Non-Material Impact - Within the past two (2) years, the assessor made no greater than a minor impact on the OSA's cybersecurity and/or data protection program, where the assessor performed a limited scope of work with minimal impact on tactical-focused cybersecurity and/or data protection controls.

Justification: Assessors operate from a position of trust and authority. Therefore, the integrity of an assessor must be sufficiently independent of the OSA and maintain the ability to conclude on the design and operational quality of the controls assessed without bias from prior knowledge of the OSA's cybersecurity and privacy control structure. An actual or perceived COI devalues an assessor's integrity. In a worst-case scenario, when there is an actual COI, the assessment results could be considered fraud if the assessor benefits from the activity.

Guidance: Avoiding COI may be achieved through:

- *Being aware of what constitutes a material and non-material impact; and*
- *Due diligence practices for assessment team participation reviews.*

3PAAC Standard 2: Secure Practices

SCF 3PAOs must identify potential assessment-related threats and implement ways to minimize and/or mitigate those associated risks.

Justification: SCF Assessors and SCF 3PAOs must be capable of protecting data at a level equivalent to the assessed environment. This requires the assessors and SCF 3PAOs to proactively identify relevant threats and implement appropriate cybersecurity and/or data protection controls to minimize risk to the SCF 3PAO and OSA.

Guidance: The SCF 3PAO is expected to define and implement pertinent cybersecurity and/or data protection controls required by applicable laws, regulations, contractual obligations and industry norms.

3PAAC Standard 2.1: Security & Data Protection By Design & By Default

SCF 3PAOs must implement security and data protection by design and by default principles for governing:

1. **Administrative processes;**
2. **Technology selection and architectural decisions;**
3. **Physical security practices; and**
4. **The protection of sensitive and/or regulated data throughout the information lifecycle.**

Justification: Cybersecurity and data protection practices need to be "baked in" as compared to "bolted on" a SCF 3PAO's day-to-day practices. This is the concept of cybersecurity and data protection practices being consciously "designed and implemented" to ensure secure and compliant practices are operationalized across system and information lifecycles.

Guidance: The Secure Controls Framework (SCF) has Cybersecurity & Data Privacy by Design (C|P) Principles that SCF 3PAOs can leverage.[48] The term "sensitive data" includes, but is not limited to:

- *Personal Data (PD):*
  - *Full name;*
  - *Date of birth;*
  - *Email address;*
  - *Phone number;*
  - *IP address;*
  - *Place of birth; and*
  - *Employment information.*
  - *Non-precise geographical data (e.g., ZIP code, city, state, country, etc.).*
- *Sensitive Personal Data (sPD):*
  - *Government-issued ID information (e.g., driver's license, passport, Social Security number (SSN), etc.);*
  - *Information that allows account access:*
    - *Account log-in, financial account, debit card or credit card number in combination with:*
    - *Any required security or access code, password or credentials allowing access.*
  - *Precise geolocation data;*
  - *Race or ethnicity;*
  - *Citizenship or immigration status;*
  - *Religious or philosophical beliefs;*
  - *Trade union membership;*
  - *Genetic data;*
  - *Biometric data;*
  - *Health-related data;*
  - *Data concerning a person's sex life or sexual orientation;*
  - *Contents of a data subject's communications (e.g., email and/or text messages) unless the data processor is the intended recipient of the communication;*
  - *Attorney-Client Privilege Information (ACPI); and*
  - *Cardholder Data (CHD).*
- *Intellectual Property (IP):*
  - *Patents;*

[48] *SCF C|P Principles - https://securecontrolsframework.com/domains-principles/*

- *Trade secrets;*
- *Trademarks; and*
- *Copyrights.*

- *Regulated data:*
  - *Controlled Unclassified Information (CUI);*
  - *Federal Contract Information (FCI);*
  - *Export-Controlled Data (ITAR / EAR);*
  - *Protected Health Information (PHI);*
  - *Student Educational Records (FERPA); and*
  - *Critical Infrastructure Information (CII).*

3PAAC Standard 2.2: Statement of Work (SOW)

SCF 3PAOs must formalize an agreement detailing the scope, nature and extent of the assessment that includes the following:

(1) The type of assessment to be performed, inclusive of control testing procedures;
(2) The assessment boundary;
(3) The timeline for completing each stage of work, inclusive of review and report finalization details; and
(4) Where remediation and reassessment are necessary, the reassessment stage.

Justification: A formal contract is reasonably expected to detail the nature of the work and milestones.

Guidance: SCF 3PAOs are expected to have formal onboarding processes for an OSA. This may include multiple types of agreements, in addition to a SOW:

- *Master Services Agreement (MSA);*
- *Non-Disclosure Agreements (NDAs); and*
- *Change Orders.*

3PAAC Standard 2.3: Assessment-Specific Data Protection Impact Assessment (DPIA)

SCF 3PAOs must perform a Data Protection Impact Assessment (DPIA) to cover the types of sensitive and/or regulated data that is reasonably expected to be stored, processed and/or transmitted throughout the lifecycle of the assessment.

Justification: A DPIA is designed to systematically analyze, identify and mitigate data protection risks associated with a project or initiative. A DPIA:

- *Can be used for more than data protection considerations; and*
- *Applies to multiple types of sensitive and/or regulated data.*

Guidance: Assessments should be considered discrete projects with unique data protection requirements. To understand data handling requirements, a DPIA should be performed prior to initiating any 3PAAC Services.

3PAAC Standard 2.4: Intellectual Property (IP) Protections

SCF 3PAOs must take all reasonable precautions to protect the confidentiality of all OSA Intellectual Property (IP) the assessment team is exposed to during the assessment lifecycle.

Justification: Assessors and SCF 3PAOs operate from a position of trust and authority. Therefore, assessors and SCF 3PAOs are expected to protect IP with all reasonable technical, administrative and physical controls necessary.

Guidance: The SCF 3PAO should implement a process to identify IP types that the assessment team will reasonably be exposed to. Ideally, specific systems/applications/networks containing sensitive information should be documented for awareness by the assessment team.

3PAAC Standard 2.5: Protection of Assessment Information

SCF 3PAOs must implement reasonable technical, administrative and physical controls to protect the confidentiality, integrity and availability of assessment information throughout the lifecycle of the assessment.

Justification: Assessors and SCF 3PAOs operate from a position of trust and authority. Therefore, assessors and SCF 3PAOs are expected to protect assessment-related data with all reasonable technical, administrative and physical controls necessary for the entire lifecycle of the assessment data.

Guidance: The SCF 3PAO is expected to govern its cybersecurity and/or data protection controls to protect assessment-related information. At a minimum, these reasonable controls should adhere to the applicable laws, regulations, contractual obligations and industry norms for cybersecurity and data protection protections.

SCF 3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment related:[49]

- *Data handling:*
  - *Data collection;*
  - *Data storage;*
  - *Data transmission; and*
  - *Data destruction; and*
- *Post-testing activities:*
  - *Mitigating recommendations;*
  - *Reporting; and*
  - *Remediation/mitigation.*

3PAAC Standard 2.6: Use of Assessment Information

SCF 3PAOs are prohibited from using information obtained during an assessment for any purpose not:

(1) Explicitly authorized by the OSA; and
(2) Included in the MSA or SOW.

Justification: Assessors and SCF 3PAOs operate from a position of trust and authority. Therefore, assessors and SCF 3PAOs are expected to use the collected information only for the assessment's stated purpose(s).

Guidance: The MSA/SOW and DPIA should clearly define permissible uses of assessment information, including any limitations on data sharing and requirements for data anonymization. Explicit clauses should prohibit using data for purposes outside the agreed scope.

3PAAC Standard 2.7: Disposal of Assessment Information

SCF 3PAOs must:

(1) Satisfy statutory, regulatory and/or contractual obligations for data retention;
(2) Adhere to a formal data retention schedule; and
(3) Securely dispose of assessment information, once the minimum retention period is achieved.

Justification: SCF 3PAOs operate from a position of trust and authority. Therefore, SCF 3PAOs are expected to securely dispose of assessment-related data once the data retention period is met, as agreed to in the SOW and/or MSA.

Guidance: For assessments not involving sensitive and/or regulated data, or an OSA with specific retention requirements, it is reasonable for a SCF 3PAO to maintain an OSA's assessment data for no less than three (3) years. For regulated OSAs, suggestions are as follows:

- *Health Insurance Portability and Accountability Act (HIPAA) requires Covered Entities (CEs) and Business Associates (BAs) to retain certain documents for a minimum of six (6) years;*
- *Accounting and assessment firms generally follow the Institute of Internal Auditors (IIA) and US-based tax authority guidance of seven (7) years; and*

[49] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

- *The rule for Cybersecurity Maturity Model Certification (CMMC) requires CMMC Third-Party Assessment Organizations (C3PAOs) to retain assessment-related information for a minimum of six (6) years.*[50]

Based on the DPIA and contractual obligations as part of the assessment, the SCF 3PAO may have unique retention requirements for assessment findings. Each assessment must have a discrete and secure storage location, with the capability to manually, or automatically, purge assessment information once the data retention period is met.

3PAAC Standard 2.8: Sampling Methodology

SCF 3PAOs must define the specific sampling methodology used to perform 3PAAC Services. Acceptable sampling methods include:

(1) Statistical; or
(2) Nonstatistical.

Justification: SCF 3PAOs operate from a position of trust and authority. Therefore, SCF 3PAOs are expected to be able to explain the methods used to determine sufficient sampling in order to defend its assessment findings against People, Processes, Technologies, Data and Facilities (PPTDF).

Guidance: Statistical sampling uses random selection to draw conclusions about a population, while non-statistical sampling uses judgment to select a sample:

- *Statistical sampling includes, but is not limited to:*
  - *Random selection (e.g., random number generators); and*
  - *Linear systematic sampling; and*
  - *Circular systematic sampling.*
- *Nonstatistical sampling includes, but is not limited to:*
  - *Haphazard sampling;*
  - *Judgement sampling; and*
  - *Block sampling.*

For industry references:

- *NIST SP 800-53A: Provides guidelines for assessing the effectiveness of security controls. It includes specific procedures for evidence collection and analysis (e.g., examine, interview and test).*
- *NIST SP 800-115: Offers technical information security testing and assessment guidelines, including evidence sampling techniques.*

The sampling methodology should be able to address the following questions:

(1) What question is being answered? (e.g., underlying rationale for collecting the evidence).
(2) What data elements are being collected?
(3) Is the data element continuous or discrete?
  a. Continuous data is data that can take any value within a given range and can be measured with increasing precision; and
  b. Discrete data is data that can only take on specific, separate values, often whole numbers, and cannot be subdivided or measured.
(4) Who will be performing the data collection?
(5) What is the source and format of the data?
(6) Are there related conditions to record? (e.g., other information that should be recorded to understand or explain the data).
(7) How frequently will the data be collected, if more than one (1) iteration of sampling is performed?
(8) What steps are used to eliminate bias to protect the integrity of the data collection?
(9) How the data will be displayed once it is collected and analyzed?

Within cybersecurity assessments, haphazard sampling is commonly used where an assessor makes a random selection without bias or any specific reason to include or omit from the sample population. This requires looking at evidence populations according to:

[50] *CFR Part 170.17(c)(4) - https://www.federalregister.gov/d/2024-22905/p-2279*

- *Standardized; or*
- *Non-Standardized*

To help explain the differences between a standardized vs a non-standardized population:

- *Technology assets (e.g., servers, routers, switches, laptops, etc.) are likely built according to an organization-approved hardening standard. This creates a standardized population, where configurations can be quickly assessed at scale with appropriate tools.*
- *Processes (e.g., risk assessments, onboarding/offboarding actions, etc.) should follow standardized procedures. Mature processes form a standardized population, where practices can be assessed against a documented procedure.*
- *Data (e.g., PII, CHD, CUI, ePHI, etc.) should be properly categorized/classified. Managed data sets form a standardized population, where data can be assessed at scale with appropriate tools (assuming it is properly categorized).*
- *People (e.g., employees, contractors, etc.) are unique, where you may have various work schedules, assigned work locations, etc. People form a non-standardized population, where a sample size may need to be larger than a standardized sample size, due to a lack of standardization.*
- *Facilities (e.g., offices, warehouses, data centers, franchise locations, etc.) are often unique, based on geographic location and the physical footprint an operation may be forced to conform to. Similar to people, facilities form a non-standardized population, where a sample size may need to be larger than a standardized sample size, due to a lack of standardization.*

From a PPTDF perspective, the CDPAS guidance on haphazard sampling is:

Standardized Population (Process, Technology or Data)	Recommended Minimum Sample Size
≥ 100	5% or 20 (smaller of the two values)
21 - 99	5%
≤ 20	10%

Non-Standardized Population (People or Facilities)	Recommended Minimum Sample Size
≥ 100	2% or 10 (larger of the two values)
21 - 99	10% or 3 (larger of the two values)
≤ 20	30% or 1 (larger of the two values)

There are four (4) factors that impact sample sizes:

(1) Data type. Discrete data requires larger sample sizes than continuous data.
(2) Required confidence level. The sample size requirement increases as confidence level increases.
(3) Margin of error. The sample size requirement increases as margin of error decreases.
(4) Variation in the population or process. The sample size requirement increases as standard deviation or proportion increases.

3PAAC Standard 3: Due Diligence - OSAs

OSA must:

(1) Identify, document and remediate risks in accordance with the OSA's documented risk management practices;
(2) Perform due diligence activities in preparation for an assessment;
(3) Document these activities as part of the OSA's assessment planning process; and
(4) Demonstrate evidence of assessment readiness to a SCF 3PAO for 3PAAC Services.

Justification: The OSA has a fiduciary duty to its shareholders. Being unprepared to engage with a SCF 3PAO for 3PAAC Services is fiscally irresponsible, since 3PAAC Services are costly and the likelihood of a successful assessment without evidence of due diligence is remote.

Guidance: OSAs can use ISO 27005[51] or NIST SP 800-37[52] for guidance on implementing and maintaining its risk management practices.

OSAs should treat assessments as discrete projects. This proper resourcing and governance can help an OSA perform and document due diligence activities.

The NIST Risk Management Framework (RMF) defines the lifecycle of cybersecurity & data protection controls.[53] The RMF consists of seven (7) unique phases that cover the lifecycle of controls governance:

(1) Prepare. Essential activities to prepare the OSA to manage cybersecurity and privacy risks;
(2) Categorize. Categorize systems, applications, services and data based on an impact analysis;
(3) Select. Select appropriate cybersecurity and data protection controls to protect PPTDF *based on risk assessments;*
(4) Implement. Implement cybersecurity and data protection controls and document how those controls are deployed;
(5) Assess. Assess to determine if the cybersecurity and data protection controls are in place, operating as intended, and producing the desired results;
(6) Authorize. A senior OSA official (e.g., manager, director, officer, etc.) makes a risk-based decision to authorize the system, application, service or project to operate in a production environment; and
(7) Monitor. Continuously monitor:
    a. Cybersecurity and data protection control implementation; and
    b. Evolving risks and threats.

In the context of 3PAAC Services, OSAs should expect a SCF 3PAO to ask reasonable questions pertaining to the following governance topics:

- *How the OSA's performs due diligence and due care activities for cybersecurity and data protection obligations;*
- *How the OSA's systems/processes/services/data are categorized;*
- *The reasoning for the OSA's cybersecurity & data protection controls that were selected;*
- *How the OSA's cybersecurity & data protection controls were implemented;*
- *The method the OSA used to assess cybersecurity & data protection controls, prior to systems/services/applications going into production; and*
- *The OSA's ongoing monitoring practices to determine:*
    - *Cybersecurity & data protection control effectiveness; and*
    - *Awareness of evolving risks and threats.*

3PAAC Standard 3.1: Adherence To Data Protection Requirements

OSA must adhere to all applicable statutory, regulatory and/or contractual obligations to protect sensitive and/or regulated data during 3PAAC Services.

Justification: Providing access to specific systems, applications, services and/or data may not be authorized, due to existing data protection practice requirements (e.g., privacy notice, data sharing agreements, etc.).

Guidance: OSAs should perform a DPIA to identify the types of data processed and their sensitivity levels and help systematically identify, analyze and mitigate data protection risks associated with 3PAAC Services. The DPIA should be performed before initiating any 3PAAC Services to understand potential limitations on assessor access to systems, applications, services and/or data.

3PAAC Standard 3.2: Assessment Boundary Demarcation

OSA must:

(1) Establish the scope of the assessment by defining the assessment boundary demarcation as:
    a. Organization-wide;
    b. A specific contract, project or initiative;
    c. A specific Business Unit (BU) within an organization; or

[51] *ISO 27005 - https://www.iso.org/standard/80585.html*
[52] *NIST SP 800-37 - https://csrc.nist.gov/pubs/sp/800/37/r2/final*
[53] *NIST RMF - https://csrc.nist.gov/projects/risk-management/about-rmf*

d. **A specific country, or geographic region, of the organization's business operations; and**

(2) If applicable, identifying relevant third-parties that make up the assessment boundary.

Justification: The OSA is ultimately responsible for conducting the due diligence to define the assessment boundary demarcation. This fundamental step influences the SOW for 3PAAC Services.

Guidance: To define the demarcation of the assessment boundary:

- *For an organization-wide scope, it is defined by a discrete:*
  - *Taxpayer Identification Number (TIN);*
  - *Employer Identification Number (EIN);*
  - *Value Added Tax (VAT);*
  - *Dun & Bradstreet Data Universal Numbering System (DUNS); or*
  - *If applicable, a Commercial And Government Entity (CAGE) Code.*
- *For a contract, project, product or initiative, it is defined by:*
  - *Sufficient detail to describe the scope of the assessment boundary:*
    - *People;*
    - *Processes;*
    - *Technologies;*
    - *Data; and*
    - *Facilities;*
  - *Contract number and/or the name of the project or initiative; and*
  - *If applicable, a CAGE Code that is associated with the contract.*
- *For a BU, country or geographic region, it is defined by:*
  - *Sufficient detail to describe the scope of the assessment boundary:*
    - *People;*
    - *Processes;*
    - *Technologies;*
    - *Data; and*
    - *Facilities;*
  - *OSA-designated name for the BU, country(ies) or geographic region; and*
  - *If applicable, a CAGE Code that is associated with the BU.*

3PAAC Standard 3.3: Graphical Representation of Assessment Boundary

OSA must generate a graphical representation of the assessment boundary to ensure control applicability is appropriately determined for systems, applications, services and third-parties that:

(1) Reflects the current architecture of the network environment(s);

(2) Clearly represents network access points on the perimeter of the network(s);

(3) Documents all sensitive and/or regulated data flows; and

(4) Contains sufficient detail to assess the applicable cybersecurity and/or data protection controls.

Justification: Graphically representing the assessment boundary helps:

- *Prevent miscommunication among stakeholders by providing a clear visual delineation of which systems, data and processes are included within the scope; and*
- *Ensure comprehensive coverage by reducing errors in scoping and including all relevant elements during the assessment.*

Guidance: A graphical representation of the assessment boundary can be in the form of a network diagram.

3PAAC Standard 3.4: Stakeholder Identification

OSA must clearly define applicable internal and third-party assessment stakeholders.

Justification: Identifying the applicable internal and external stakeholders is crucial to any assessment-related due diligence. Developing a trust relationship with key stakeholders is also essential for a successful assessment.

Guidance: Stakeholder identification can be achieved through documenting a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix:

- *Responsible - entity directly responsible for performing a task (e.g., control/process operator);*
- *Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner);*
- *Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task;*
- *Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and*
- *Informed - entity(ies) not involved in task execution but are informed when the task is completed.*

3PAAC Standard 3.5: Control Reciprocity

For control reciprocity:

(1) The sole authority to determine control reciprocity is the:
- **a. Certification scheme owner; or**
- **b. Applicable Accreditation Body (AB); and**

(2) If a control reciprocity exists:
- **a. OSA must identify the specific controls it seeks reciprocity for; and**
- **b. Applicable controls identified for reciprocity must share the same assessment boundary(ies).**

Justification: Control reciprocity decisions involve an analysis to determine applicability, which is solely up to the discretion of an authoritative body to make the determination. OSA, assessor and/or SCF 3PAO opinions do not matter in control reciprocity decisions, since they are non-authoritative.

Guidance: For properly scoped and applicable controls, SCF 3PAOs are required to accept the reciprocity decision from the authoritative body.

Control reciprocity decisions are rarely straightforward, due to the nature of crosswalk mapping between different frameworks. Clarification should be sought from the relevant authoritative body for answers to specific reciprocity questions.

Example 1: Cybersecurity Maturity Model Certification (CMMC)

- *An OSA with a current and valid CMMC Level 2 certification would be able to demonstrate conformity with:*
  - *Controlled Unclassified Information (CUI) controls in NIST SP 800-171 R2; and*
  - *Federal Contract Information (FCI) controls in FAR 52.204-21 and NIST SP 800-171 R2.*
- *While the OSA would be able to demonstrate compliance with CUI and FCI controls, it would not be able to demonstrate conformity with broader compliance obligations for:*
  - *DFARS 252.204-7012 (e.g., incident reporting requirements); and/or*
  - *Non-Federal Organization (NFO) controls from NIST SP 800-171 R2.*

Example 2: FedRAMP

- *A current and valid FedRAMP certification would allow an OSA to demonstrate conformity with applicable NIST SP 800-53 in the FedRAMP Cloud Service Provider (CSP) environment.*
- *The OSA would not be able to use that same FedRAMP certification to demonstrate conformity with applicable NIST SP 800-53 controls outside of the FedRAMP CSP environment.*

Example 3: ISO/IEC 27001

- *A current and valid ISO/IEC 27001:2022 certification would allow an OSA to demonstrate conformity with applicable ISO/IEC 27001:2022 controls within the scope of the ISO/IEC 27001:2022 certification.*
- *The OSA would not be able to use that same ISO/IEC 27001:2022 certification to demonstrate conformity with controls outside of the scope of the ISO/IEC 27001:2022 certification.*

3PAAC Standard 3.6: Control Inheritance

To claim control inheritance:

(1) From the External Services Provider (ESP) the OSA is seeking control inheritance, the OSA must obtain evidence in the form of a:
- **a. First-Party Declaration (1PD); or**

   b. **Third-Party Attestation (3PA);**
(2) **OSA must identify the specific controls it seeks control inheritance for;**
(3) **Applicable controls identified for control inheritance must share the same assessment boundary(ies); and**
(4) **The ESP's service(s) claiming control inheritance must be documented in:**
   a. **A contract between the OSA and ESP; and**
   b. **A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls.**

Justification: It is reasonable to assume that OSAs will have external support and/or services, which requires the evaluation of inherited controls.

Guidance: It is at the SCF 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.

Example 1: Service Organization Control (SOC) 2 Type 2

- *An OSA could leverage an ESP's Service Organization Control (SOC) 2 Type 2 report to address physical security of data center assets.*
- *The OSA would not be able to leverage that same SOC 2 Type 2 report for the OSA's on-premises physical security.*

Example 2: Cybersecurity Maturity Model Certification (CMMC)

- *An OSA with a current and valid CMMC Level 2 certification would be able to demonstrate conformity with:*
  - *Controlled Unclassified Information (CUI) controls in NIST SP 800-171 R2; and*
  - *Federal Contract Information (FCI) controls in FAR 52.204-21 and NIST SP 800-171 R2.*
- *While the OSA would be able to demonstrate compliance with CUI and FCI controls, it would not be able to demonstrate conformity with broader compliance obligations for:*
  - *DFARS 252.204-7012 (e.g., incident reporting requirements); and/or*
  - *Non-Federal Organization (NFO) controls from NIST SP 800-171 R2.*

3PAAC STANDARD 3.7: STATEMENT OF APPLICABILITY (SOA) - DEFINED CYBERSECURITY AND/OR DATA PRIVACY CONTROLS

OSA must define a Statement of Applicability (SoA) that identifies applicable cybersecurity and/or data protection controls that apply to the organization.

Justification: The OSA is ultimately responsible for conducting the due diligence to define the applicable cybersecurity and/or data protection controls for the assessment. This fundamental step influences the SOW for 3PAAC Services.

Guidance: The SCF's Integrated Controls Management (ICM) Model provides guidance on how to properly define applicable controls.[54] The ICM focuses on the need to understand and clarify the difference between "compliant" versus "secure" since the distinction is necessary to have coherent risk management discussions. To assist in this process, an organization's applicable controls can be categorized according to "must have" vs "nice to have" requirements:

- *Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.*
- *Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and/or data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments. DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.*

The combination of MCR and DSR equate to an organization's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements for PPTDF in one control set. It describes the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity and data protection perspective. In short, the MSR can be considered an organization's IT General Controls (ITGC), which establishes the basic controls that must be applied to systems, applications,

[54] *Integrated Controls Management (ICM) Model - https://securecontrolsframework.com/integrated-controls-management/*

services, processes and data throughout the enterprise. ITGC provide the foundation of assurance for an organization's decision makers. ITGC enables an organization's governance function to define how technologies are designed, implemented and operated.

3PAAC Standard 3.8: Defined Risk Tolerance

OSA must define their organizational risk tolerance as one (1) of the five (5) following levels:

1. **Low;**
2. **Moderate;**
3. **High;**
4. **Severe; or**
5. **Extreme.**

Justification: Defined risk tolerance provides criteria to assess an OSA's risk management practices. An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- *Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices);*
- *Organization-specific threats (natural and manmade);*
- *Reasonably expected industry practices;*
- *Pressure from competition; and*
- *Executive management decisions (e.g., Board of Directors).*

Guidance: See Appendix B: Risk Terminology Normalization for context and examples for determining the appropriate risk tolerance for an organization.

3PAAC Standard 3.9: Defined Maturity Level

OSA must define the current and targeted level of maturity of its cybersecurity and/or data protection program as one (1) of the following six (6) designations:

1. **Level 0 - Not Performed;**
2. **Level 1 - Performed Informally;**
3. **Level 2 - Planned & Tracked;**
4. **Level 3 - Well-Defined;**
5. **Level 4 - Quantitatively-Controlled; or**
6. **Level 5 - Continuously Improving.**

Justification: The intended usage of maturity is meant to provide relevant context, as it pertains to control implementation and operations. Different evaluation criteria would be reasonably expected for each level of maturity.

Guidance: The CDPAS leverages the maturity levels from the SCF's Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM):[55]

- ***LEVEL 0 MATURITY - NOT PERFORMED** This level of maturity is defined as "non-existence practices," where the control is not being performed:*
  - *Practices are non-existent, where a reasonable person would conclude the control is not being performed.*
  - *Evidence of due care and due diligence do not exist to demonstrate compliance with applicable statutory, regulatory and/or contractual obligations.*
- ***LEVEL 1 MATURITY - PERFORMED INFORMALLY** This level of maturity is defined as "ad hoc practices," where the control is being performed, but lacks completeness & consistency:*
  - *Practices are "ad hoc" where the intent of a control is not met due to a lack consistency and formality.*
  - *When the control is met, it lacks consistency and formality (e.g., rudimentary practices are performed informally).*
  - *A reasonable person would conclude the control is not consistently performed in a structured manner.*

[55] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*

- *Performance depends on the specific knowledge and effort of the individual performing the task(s), where the performance of these practices is not proactively governed.*
- *Limited evidence of due care and due diligence exists, where it would be difficult to legitimately disprove a claim of negligence for how cybersecurity/privacy controls are implemented and maintained.*

- ***LEVEL 2 MATURITY - PLANNED & TRACKED*** *Practices are "requirements-driven" where the intent of control is met in some circumstances, but not standardized across the assessment boundary:*
  - *Practices are "requirements-driven" (e.g., specified by a law, regulation or contractual obligation) and are tailored to meet those specific compliance obligations (e.g., evidence of due diligence).*
  - *Performance of a control is planned and tracked according to specified procedures and work products conform to prescribed standards (e.g., evidence of due care).*
  - *Controls are implemented in some, but not all applicable circumstances/environments (e.g., specific enclaves, facilities or locations).*
  - *A reasonable person could conclude controls are "compliance-focused" to narrowly meet a specific obligation, since the control(s):*
    - *Are localized to specific systems, applications and/or services; and*
    - *Are not standardized across the authorization boundary.*
  - *Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.*
- ***LEVEL 3 MATURITY - WELL DEFINED*** *This level of maturity is defined as "standardized practices," where the control implementation is well-defined and standardized across the assessment boundary:*
  - *From the perspective of the CDPAS, Level 3 maturity practices are standardized across the Assessment Boundary, where this could be across:*
    - *The entire organization;*
    - *A specific contract, project or initiative;*
    - *A specific Business Unit (BU) within an organization; or*
    - *A specific country, or geographic region, of the organization's business operations.*
  - *Controls are implemented in all applicable circumstances/environments (deviations are documented and justified).*
  - *Performance of a control is according to specified well-defined and standardized procedures.*
  - *Control execution is planned and managed using an enterprise-wide, standardized methodology.*
  - *Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.*
- ***LEVEL 4 MATURITY - QUANTITATIVELY CONTROLLED*** *This level of maturity is defined as "metrics-driven practices," where in addition to being well-defined and standardized control implementation across the assessment boundary, there are detailed metrics to enable governance oversight:*
  - *Practices are "metrics-driven" and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement.*
  - *Practices build upon established Level 3 maturity criteria and have detailed metrics to enable governance oversight.*
  - *Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance.*
  - *Performance is objectively managed and the quality of work products is quantitatively known.*
- ***LEVEL 5 MATURITY - CONTINUOUSLY IMPROVING*** *This level of maturity is defined as "world-class practices," where control implementation is not only well-defined and standardized across the organization (with detailed metrics), processes are continuously improving:*
  - *Practices are "world-class" capabilities that leverage predictive analysis.*
  - *Practices build upon established Level 4 maturity criteria and are time-sensitive to support operational efficiency, which likely includes automated actions through machine learning or Artificial Intelligence (AI).*
  - *Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.*
  - *Process improvements are implemented according to "continuous improvement" practices to affect process changes.*

3PAAC Standard 3.10: Defined Materiality Threshold

OSA must define the criteria for materiality, as it pertains to its cybersecurity and data protection program.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. Materiality designations are intended to act as a "guard rail" for risk management decisions. A material weakness crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: The SCF Council defines the materiality threshold for an organization's cybersecurity and data protection program as, "A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance." [56]

Publicly traded companies regulated by the US Security and Exchanges Commission (SEC) must disclosures "material cybersecurity incidents" on Form 8-K, Item 1.05(a).[57] A financial benchmark is commonly used to determine materiality. Materiality goes beyond SEC Form 8-K filings and is valuable for the broader concept of risk management practices, since it helps an organization clearly understand what is important versus what is not important. Prioritization is key in risk management and determining materiality thresholds is a tool that should be utilized.

Generally, account criteria from pre-tax income, total assets, total revenue and total equity to provide options for both "single criteria determinations" and "averaged determinations" to establish objective thresholds. From a financial benchmark perspective, for something to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one, or more, of the following criteria where the potential financial impact is measured as:[58]

- *≥ 5% of pre-tax income*
- *≥ 0.5% of total assets*
- *≥ 1% of total equity (shareholder value); and/or*
- *≥ 0.5% of total revenue.*

3PAAC Standard 3.11: Material Risk Designation

OSA must:

(1) Identify risks from its risk catalog that have the potential to pose a material impact; and

(2) Designate those identified risks as material risks.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material risk crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: See Appendix B: Risk Terminology Normalization for context on risk management concepts. A risk is:

- *Where someone or something valued is exposed to danger, harm or loss (noun); or*
- *To expose someone or something valued to danger, harm or loss (verb).*

When there is an identified risk that poses a material impact, that is a material risk:

- *A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., potential class action lawsuit, death related to product usage, etc.); and*
- *A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.*

[56] SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/
[57] SEC Form 8-K - https://www.sec.gov/files/form8-k.pdf
[58] Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf

3PAAC Standard 3.12: Material Threat Designation

OSA must:

(1) Identify threats from its threat catalog that have the potential to pose a material impact; and

(2) Designate those identified risks as material threats.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material threat crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: A threat:

- *Is a person or thing likely to cause damage or danger (noun); or*
- *Indicates impending damage or danger (verb).*

When there is an identified threat that poses a material impact, that is a material threat:

- *A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and*
- *A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.*

3PAAC Standard 3.13: Material Incident Designation

OSA must:

(1) Identify reasonable incidents that have the potential to pose a material impact; and

(2) Designate those identified risks as material incidents.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material incident crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: An incident is an occurrence that actually or potentially:

- *Jeopardizes the Confidentiality, Integrity, Availability or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits; and/or*
- *Constitutes a violation or imminent threat of violating an organization's policies, procedures or acceptable use practices.*

When there is an incident that poses a material impact, that is a material incident:

- *A material incident is an occurrence that does or has the potential to:*
  - *Affect the CIAS of systems, applications, services or data; or*
  - *Violate organizational practices that have a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.); and*
- *Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate processes to identify, respond to and recover from such incidents.*

3PAAC Standard 3.14: Internal Assessment

To demonstrate evidence of assessment readiness for 3PAAC Services to a SCF 3PAO, OSA must:

(1) Perform at least one (1) internal cybersecurity and/or data protection controls assessment in preparation for an external assessment by a SCF 3PAO; and

(2) Document the internal assessment(s) as part of the OSA's assessment preparation process.

Justification: Performing internal assessments to demonstrate readiness for 3PAAC Services is a due diligence activity. The OSA has a fiduciary duty to its shareholders. Being unprepared to engage with a SCF 3PAO for 3PAAC Services is fiscally irresponsible, since 3PAAC Services are costly and the likelihood of a successful assessment without evidence of due diligence is remote.

Guidance: OSAs should perform and document internal assessments with the same level of rigor and reasonable interpretation of controls expected from a SCF 3PAO.

3PAAC Standard 3.15: Implemented Capability

To be considered an Implemented Capability (IC) and be assessable by a SCF 3PAO, an OSA's:

(1) Technology capabilities will only be considered implemented if the system(s), application(s) and/or service(s) has/have been operational in a production environment for at least sixty (60) days;

(2) Administrative processes will only be considered implemented if there is evidence to demonstrate that process has been:

a. Used in a real-world situation (e.g., onboarding/offboarding personnel, incident response, etc.); and/or

b. Formally tested (e.g., documented incident response exercise); and

(3) Physical capabilities will only be considered implemented if the physical security mechanism(s) has/have been operational in a production environment for at least thirty (30) days.

Justification: It takes time for a control to be in place before it can legitimately be verified as being both employed and operational, where the control is operating as intended. This is applicable to technologies, administrative processes and physical security mechanisms.

Guidance: An Implemented Capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.

3PAAC Standard 4: Due Diligence - Assessors & SCF 3PAOs

SCF 3PAOs must:

(1) Perform due diligence activities in preparation for an assessment;

(2) Document these activities as part of the SCF 3PAO's assessment planning process; and

(3) Include the justification for accepting the OSA's readiness for 3PAAC Services.

Justification: Due diligence is simply taking reasonable steps to avoid harm. Therefore, SCF 3PAOs must perform due diligence activities for all assessments.

Guidance: Treating assessments as discrete projects can help a SCF 3PAO perform and document due diligence activities, since many activities are commonly expected for engagements.

3PAAC Standard 4.1: Formalized Assessment Plan

SCF 3PAOs must:

(1) Formalize OSA-specific assessment plans; and

(2) Designate an Assessment Team Lead (ATL) with assigned responsibilities to conduct 3PAAC Services.

Justification: It is a reasonable expectation for SCF 3PAOs to present a formalized assessment plan to the OSA.

Guidance: Treating assessments as discrete projects can help a SCF 3PAO perform and document due diligence activities, since these activities are commonly expected for assessment engagements. Adequately formulating the plan includes formal documentation of fieldwork steps that reasonably support execution of the SCF 3PAO's assessment methodology from fieldwork initiation to completion, including report development, peer review and issuance.

SCF 3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment execution:[59]

- *Security assessment planning:*
  - *Developing a security assessment policy;*
  - *Prioritizing and scheduling assessments;*
  - *Selecting and customizing techniques;*

[59] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

- *Assessment logistics:*
  - *Assessor selection and skills;*
  - *Location selection; and*
  - *Technical tools and resources selection;*
- *Assessment plan develop; and*
- *Legal considerations;*

- *Security assessment execution:*
  - *Coordination;*
  - *Assessing;*
  - *Analysis; and*
  - *Data handling:*
    - *Data collection;*
    - *Data storage;*
    - *Data transmission; and*
    - *Data destruction; and*
- *Post-testing activities:*
  - *Mitigating recommendations;*
  - *Reporting; and*
  - *Remediation/mitigation.*

DODM 8140.03 should be used for competence criteria for the role of an ATL. Based on the position category and seniority for the role, the ATL is expected to be an "senior-level SCF Assessor" with the following qualifications:[60]

- *An undergraduate degree:*
  - *From an:*
    - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
    - *Centers of Academic Excellence (CAE) designated institution; and*
  - *In the one of the following degrees:*
    - *Information Technology (IT)*
    - *Cybersecurity;*
    - *Data Science;*
    - *Information Systems; or*
    - *Computer Science (CS);*

and/or

- *One (1) of the following certifications:*
  - *CISM - ISACA Certified Information Security Manager;*
  - *CISA - ISACA Certified Information Systems Auditor;*
  - *CISSP - ISC2 Certified Information Systems Security Professional;*
  - *CISSP-ISSEP - ISC2 CISSP - Information Systems Security Engineering Professional;*
  - *GCSA - GIAC Cloud Security Automation;*
  - *GSLC - GIAC Security Leadership Certification;*
  - *GSNA - GIAC Systems and Network Auditor;*
  - *CySA+ - CompTIA Cybersecurity Analyst plus;*
  - *C)ISSO - Certified Information Systems Security Officer;*
  - *C)PTE - Certified Penetration Testing Engineer; and/or*
  - *FITSP-A - Federal IT Security Professional-Auditor.*

3PAAC Standard 4.2: Defined Assessment Boundaries

SCF 3PAOs must:

(1) Validate the scope of the assessment by defining assessment boundaries; and

(2) Limit assessor activities to the defined assessment boundary.

[60] *DoDM 8140.03 - https://public.cyber.mil/wid/dod8140/qualifications-matrices/*

Justification: Assessors and SCF 3PAOs operate from a position of trust and authority. Therefore, assessors must recognize the boundary and restrict assessment activities to systems, applications, services, personnel and third parties within that defined boundary.

Guidance: The Unified Scoping Guide (USG) provides a methodology to assist SCF 3PAOs with: [61]

- *Validating control boundaries; and*
- *Defining the scope of the sensitive and/or regulated data where it is stored, transmitted and/or processed.*

3PAAC Standard 4.3: Validate Control Applicability

SCF 3PAOs must ensure applicable cybersecurity and/or data protection controls to be assessed are:

(1) Applicable to the scope of the SOW; and
(2) Validated by the OSA.

Justification: OSA must have documented evidence to justify the assessment scope to the SCF 3PAO. As part of due diligence activities, SCF 3PAOs need to know the specific cybersecurity and/or data protection controls that will make up the assessment, confined within the assessment boundary(ies).

Guidance: Documentation of an OSA's controls by the assessor on behalf of, or in conjunction with, the OSA would not be considered a COI. For the purposes of completing the assessment, this clarification of applicable controls would not constitute "control design or implementation" services.

3PAAC Standard 4.4: Defined Evidence Request List (ERL)

Based on the defined cybersecurity and/or data protection controls, the assessor must provide the OSA with an Evidence Request List (ERL) that defines the SOW-specific artifacts necessary to perform 3PAAC Services. For evidence:

(1) The OSA must provide evidence artifacts of a level of detail, accuracy and formatting to satisfy assessment rigor criteria; and
(2) The SCF 3PAO may request additional evidence artifacts, or clarification of OSA-submitted ERL artifacts, as necessary to perform 3PAAC Services.

Justification: Assessors and SCF 3PAOs operate from a position of trust and authority. Therefore, minimizing "scope creep" that can increase the duration, cost and personnel commitments associated with an assessment is essential. As part of due diligence activities, assessors and SCF 3PAOs are expected to:

- *Define an authoritative ERL; and*
- *Before the start of the assessment, provide any artifact requests to the OSA.*

An ERL provides assessment-specific artifacts where:

- *It establishes a minimum level of reasonable evidence necessary for the SCF 3PAO to conduct 3PAAC Services;*
- *The intent is for ERLs to establish a finite list of supporting evidence used in an assessment; and*
- *Prior to the start of the assessment, an ERL will be provided by the SCF 3PAO to the OSA.*

Guidance: The SCF provides ERL that assessors and SCF 3PAOs can use. The ERL is part of the SCF download. [62] *The ERL represents the minimum level of reasonable evidence requests.*

3PAAC Standard 4.5: Explicit Authorization For Testing

Prior to performing assessment-related control testing activities, SCF 3PAOs must obtain written authorization from the OSA in the form of a:

(1) Signed contract;
(2) MSA;
(3) SOW; and/or
(4) Change order.

[61] *Unified Scoping Guide (USG) - https://unified-scoping-guide.com*
[62] *SCF Evidence Request List (ERL) - https://securecontrolsframework.com/scf-download*

Justification: Obtaining explicit authorization minimizes liability to assessors and SCF 3PAOs. The assumption is that an OSA's network is highly integrated with dependencies that can affect the ability of the organization to perform its business operations. Therefore, SCF 3PAOs must receive written authorization to perform specific assessment-related control testing activities.

Guidance: Any control testing activities should be viewed similarly to precautions taken by a third-party to perform a vulnerability assessment or penetrating testing engagement.

3PAAC Standard 4.6: First-Party Declarations (1PD) - Control Inheritance

SCF Assessors must review available 1PD artifacts to understand possible dependencies and control inheritance, if applicable and/or available. 1PDs must:

(1) Originate from internal audits and/or assessments by:
- **a. The OSA; and/or**
- **b. ESPs that impact the OSA's assessment boundary;**

(2) If applicable, document the ESP's service(s) the OSA is claiming control inheritance in:
- **a. A contract between the OSA and ESP; and**
- **b. A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls;**

(3) Contain sufficient detail to determine the applicability of inherited cybersecurity and/or data protection controls;

(4) Specify the specific controls being inherited;

(5) Validate that controls identified for inheritance share the same assessment boundary(ies);

(6) Reflect the current architecture of the OSA's network infrastructure; and

(7) Have been generated within the past twelve (12) months.

Justification: It is a reasonable assumption that an OSA will have third-party dependencies. The OSA may provide self-attestations from supporting organizations to demonstrate control implementation. 1PD may address significant control inheritance (e.g., third-party control responsibility, service providers' security certifications, etc.), but this evidence requires some form of validation by the SCF 3PAO.

Most assessments can be considered "black box" endeavors, where the assessor has no previous information on the environment being assessed. However, some assessments are "gray box" or "white box" assessments where the assessor is expected to work off previous evidence.

Guidance: It is at the SCF 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.

3PAAC Standard 4.7: Third-Party Attestations (3PA) - Control Inheritance & Reciprocity

SCF Assessors must review available 3PA artifacts to understand possible dependencies and control inheritance, if applicable and/or available. 3PA must:

(1) Be from a reputable third-party with subject matter expertise in the topic being attested to;

(2) If applicable, document the ESP's service(s) the OSA is claiming control inheritance in:
- **a. A contract between the OSA and ESP; and**
- **b. A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls;**

(3) Contain sufficient detail to determine the applicability of inherited cybersecurity and/or data protection controls;

(4) Specify the specific controls:
- **a. Being inherited; and/or**
- **b. Claiming reciprocity;**

(5) Validate that controls identified for inheritance and/or reciprocity share the same assessment boundary(ies);

(6) Reflect the current architecture of the OSA's network infrastructure; and

(7) Have been generated within the past twelve (12) months.

Justification: It is a reasonable assumption that an OSA will have third-party dependencies. The OSA may be provided with third-party attestations (e.g., SOC 2, ISO 27001, CMMC, etc.) to demonstrate control implementation. 3PA may address significant

control inheritance (e.g., third-party control responsibility, service providers' security certifications, etc.), but this evidence requires some form of validation by the SCF 3PAO.

Guidance: For properly scoped and applicable controls:

- *SCF 3PAOs are required to accept the reciprocity decision from the authoritative body; and*
- *It is at the SCF 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.*

3PAAC Standard 4.8: Stakeholder Validation

SCF Assessors must validate the applicability of pertinent assessment stakeholders, based on the OSA's provided:

(1) Assessment boundary demarcation;
(2) Graphical representation of assessment boundary(ies);
(3) RASCI matrix;
(4) Defined cybersecurity and/or data protection controls; and
(5) When applicable:
  a. 1PD and/or
  b. 3PA.

Justification: Identified stakeholders provide justification for the defined assessment boundary. If the identified stakeholders do not support the assessment boundary, there is an indication that:

- *The scope of the assessment may be incorrect;*
- *The defined cybersecurity and/or data protection controls are incorrect; and/or*
- *The identified stakeholders are incorrect.*

Guidance: Stakeholder identification can be achieved by documenting a RASCI matrix.

3PAAC Standard 5: Due Care - OSAs

OSA must perform due care activities when executing:

(1) Control design;
(2) Control implementation; and
(3) Continued operation.

Justification: Due care is the conduct a reasonable person with appropriate skills and experience, would exercise in a similar situation. Therefore, OSAs are expected to operate by a standard of care that others in the industry would reasonably follow.

Guidance: Treating assessments as discrete projects can help an OSA perform and document due care activities. This requires proactive governance on behalf of the OSA.

3PAAC Standard 5.1: Proactive Governance

OSA must assign an employee with sufficient authority and subject matter expertise to proactively govern the OSA's cybersecurity and data protection program(s).

Justification: Proactive governance is the opposite of reactive governance, where an issue or problem is addressed after it becomes a crisis. OSAs are expected to govern its cybersecurity and data protection program proactively.

Guidance: It is possible for one role to oversee both cybersecurity and data protection efforts. However, common roles associated with hierarchical authority for the cybersecurity and data protection programs include:

- *From a cybersecurity perspective for cybersecurity-related leadership:*
  - *Chief Information Security Officer (CISO); and*
  - *Director of Cybersecurity, or a comparable position.*
- *From a data protection perspective for data privacy-related leadership:*
  - *Chief Privacy Officer (CPO).*

Proactive governance is a continuous process of risk and threat identification, analysis and remediation. In addition, it also includes proactively updating policies, standards and procedures in response to emerging threats or regulatory changes.

OSAs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on:[63]

- *Review techniques:*
  - *Documentation review;*
  - *Log review;*
  - *Ruleset review;*
  - *System configuration review;*
  - *Network sniffing and;*
  - *File integrity checking; and*
- *Target identification and analysis techniques:*
  - *Network discovery;*
  - *Network port and service identification;*
  - *Vulnerability scanning; and*
  - *Wireless scanning.*

3PAAC Standard 5.2: Non-Conformity Oversight

OSA must document, assess and implement remediation actions to address instances of non-conformity, where deficiencies with:

(1) Material controls are remediated without delay; and

(2) Non-material controls are remediated according to the:

a. Risk associated with the non-conforming control; and

b. OSA's established vulnerability management and/or change management practices.

Justification: A formal methodology is necessary to provide non-conformity oversight.

Guidance: As part of proactive governance, it is expected that OSAs will encounter instances of non-conformity due to business and technology-related changes or limitations. This ongoing process of evolving cybersecurity and/or data protection practices to meet changes in business and technology requires proactive governance suitable of withstanding scrutiny by an independent third-party. Formal oversight of non-conformities is necessary to systematically identify, track and remediate gaps in cybersecurity and/or data protection controls. For example, establishing a corrective action plan with timelines and responsibilities helps ensure that identified issues are addressed promptly and effectively.

3PAAC Standard 5.3: Annual Affirmation

OSA must:

(1) Internally perform an annual assessment that validates:

a. The assessment boundary(ies) for issued certifications;

b. POA&M items are proactively managed to remediate identified deficiencies; and

c. Implemented changes are not material to the assessment boundary(ies); and

(2) Affirm the status of its cybersecurity and data protection controls continues to support its conformity designation for applicable certifications.

Justification: Annual affirmations:

- *Ensure OSAs conduct periodic checks; and*
- *Verify that unaccounted for material changes have not occurred.*

Guidance: The organization official making the annual affirmation should be the senior individual responsible for the organization's compliance requirements. This individual should:

- *Be assigned the role of monitoring compliance with applicable requirements; and*
- *Have the technical competence to understand how compliance can be objectively demonstrated.*

Per 3PAAC Standard 9, material and non-material changes are defined as:

[63] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

- *Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.*
- *Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.*

The content of the affirmation should include the following information:

- *Name, title, and contact information for the individual performing the affirmation; and*
- *An affirmation statement attesting that the OSA has implemented and continues to maintain all applicable cybersecurity and/or data protection controls relevant to PPTDF within the relevant assessment boundary.*

3PAAC Standard 6: Due Care - Assessors & SCF 3PAOs

SCF 3PAOs must perform due care activities in the execution of assessment activities.

Justification: Due care is the conduct a reasonable person with appropriate skills and experience would exercise in a similar situation. Therefore, assessors and SCF 3PAOs are expected to operate by a standard of care that others in the industry would reasonably follow.

Guidance: Treating assessments as discrete projects can help a SCF 3PAO perform and document due care activities. This requires proactive governance on behalf of the SCF 3PAO.

3PAAC Standard 6.1: Assessment Methods

SCF Assessors must:

(1) Utilize an assessment method in accordance with the SOW; and

(2) Specify one (1) of the following assessment methods:

a. Manual Point In Time (MPIT). MPIT is a traditional assessment methodology that:

i. Is relevant to a specific point in time (time at which the controls were evaluated); and

ii. Relies on the manual review of artifacts to derive a finding;

b. Automated Point In Time (APIT). APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

i. Is relevant to a specific point in time (time at which the controls were evaluated);

ii. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and

iii. The combined output of automated and manual reviews of artifacts is used to derive a finding; or

c. Automated Evidence with Human Review (AEHR). AEHR is used for ongoing, continuous control assessments:

i. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and

ii. Recurring human reviews:

1. Evaluate the legitimacy of the results from automated control assessments; and

2. Validate the automated evidence review process to derive a finding.

Justification: The SOW is expected to capture the assessment method, since that establishes the context for expected assessor involvement and related costs. The adoption of automation technologies for 3PAAC Services must be addressed to:

- *Adjust to evolving technologies available to SCF 3PAOs; and*
- *Avoid improper assumptions about control evaluation practices.*

Guidance: It is acceptable for a SCF 3PAO to offer a single assessment method (e.g., MPIT). However, SCF 3PAOs are expected to have procedures developed for each assessment method offered as part of its 3PAAC Services.

APIT and AEHR may leverage Artificial Intelligence and/or Machine Learning (AI/ML) technologies. In the case of AI/ML being used, SCF 3PAOs must be prepared to demonstrate sufficient evidence of due diligence and due care to justify the integrity of the findings and overall assessment results (e.g., evidence of validating results, test cases, etc.).

See Appendix C: Assessment Rigor for more details on how assessment methods relate to assessment rigor. At a minimum:

- *Standard rigor should be used for MPIT assessments;*
- *Enhanced rigor should be used for APIT assessments; and*
- *Comprehensive rigor should be used for AEHR assessments.*

3PAAC STANDARD 6.2: ASSESSMENT RIGOR

SCF Assessors must perform the assessment at a level of rigor in accordance with the SOW. There are three (3) levels of rigor:

(1) Level 1 Rigor: STANDARD. Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:
  a. Implemented; and
  b. Free of obvious errors.

(2) Level 2 Rigor: ENHANCED. Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
  a. The applicable controls are:
    i. Implemented; and
    ii. Free of obvious/apparent errors; and
  b. There are increased grounds for confidence that the applicable controls are:
    i. Implemented correctly; and
    ii. Operating as intended.

(3) Level 3 Rigor: COMPREHENSIVE. Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:
  a. Whether the applicable controls are:
    i. Implemented; and
    ii. Free of obvious/apparent errors;
  b. Whether there are further increased grounds for confidence that the applicable controls are:
    i. Implemented correctly; and
    ii. Operating as intended on an ongoing and consistent basis; and
  c. There is support for continuous improvement in the effectiveness of the applicable controls.

Justification: It is essential to establish the expectation for the level of rigor to be performed by the assessment team. The SOW is expected to capture the level of rigor, since that establishes the context for expected assessor involvement and related costs. At a minimum:

- *Standard rigor should be used for MPIT assessments;*
- *Enhanced rigor should be used for APIT assessments; and*
- *Comprehensive rigor should be used for AEHR assessments.*

Guidance: See Appendix C: Assessment Rigor for more details on assessment rigor. SCF 3PAOs are expected to have assessment plans developed for each level of rigor. In addition, the SCF 3PAO is expected to develop clear criteria for determining the level of rigor (Standard, Enhanced, Comprehensive) based on the OSA's needs, risk appetite and risk profile. OSAs are responsible for selecting the most appropriate level of rigor to address their unique assessment requirements.

3PAAC STANDARD 6.3: ASSESSING BASED ON CONTROL APPLICABILITY

SCF Assessors must limit their evidence examination, interviews and testing activities based on the applicability of the assessed cybersecurity and/or data protection controls. A single cybersecurity and/or data protection control primarily applies to only one (1) of the following functions:

(1) People;
(2) Processes;
(3) Technologies;
(4) Data; and/or
(5) Facilities.

Justification: Control scoping does not mean all controls apply uniformly to every asset, individual or facility. There is a common misconception that if something is "in scope" then every control will be applicable across the entire assessment boundary. This is an incorrect assumption, since the nature of a control is primarily administrative, technical or physical. This means specific controls may not apply to all assets, processes, people and locations.

Guidance: Control scoping is not the same thing as control applicability, since it is technically infeasible to apply all controls uniformly, based on control applicability:

- *Controls are primarily administrative, technical and/or physical. This means that there may be controls that are not applicable.*
- *It is possible for a control to apply across more than a single function. However, in most cases, controls apply to a single function.*

The recommended solution is to create some form of a matrix that can apply the appropriate controls to the correct PPTDF to help identify the proper scope for the implementation of controls:

- ***People** - Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).*
- ***Processes** - Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).*
- ***Technologies** - Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.).*
- ***Data** - Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).*
- ***Facilities** - Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).*

Example 1: Network firewall

- *A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.*
- *A network firewall is a device. Therefore, a network firewall is not capable of undergoing end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.*

Example 2: User awareness training

- *User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.*
- *An individual is not a device. Therefore, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.*

Example 3: Incident Response Plan (IRP)

- *An IRP is a documented process that guides incident response operations.*
- *An IRP is not an individual or technology. Therefore, an IRP cannot sign an NDA, have MFA or be patched.*

3PAAC Standard 6.4: Assessment Objectives (AOs)

SCF Assessors must evaluate controls by utilizing Assessment Objectives (AOs), when AOs are available.

Justification: AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.

Guidance: AOs provide objective criteria that each must be satisfied to legitimately determine whether the control is implemented and operating as intended. The SCF has a catalog of AOs that SCF 3PAOs can use, including:

- *SCF baseline;*
- *NIST SP 800-53A R5;*
- *NIST SP 800-171A;*
- *NIST SP 800-171A R3; and*
- *NIST SP 800-172A.*

3PAAC Standard 6.5: Control Designation

SCF Assessors must designate a status to assessed controls as follows:

(1) **There are four (4) possible designations:**
   a. **Satisfactory;**
   b. **Deficient;**
   c. **Alternative Control; or**
   d. **Not Applicable (N/A);**

(2) **Where AOs are available, for a control to be designated as Satisfactory, each of the control's applicable AOs must be designated as:**
   a. **Satisfactory;**
   b. **Alternative Control; or**
   c. **N/A; and**

(3) **If all of the following conditions exist, a control designated as Deficient may be re-evaluated during the course of the assessment and for up to ten (10) business days following the active assessment period if:**
   a. **Additional evidence:**
      i. **Is available to demonstrate the control is satisfied; and**
      ii. **Cannot change, or limit the effectiveness of, other requirements that have previously been scored Satisfactory; and**
   b. **The Report on Conformity (ROC) has not been delivered to the OSA.**

Justification: The assessed status of controls needs a standardized status designation. A standardized methodology to describe the assessed status of a control is necessary to maintain the integrity of the assessment process.

Guidance: In the context of control designations, a designation of:

- *Satisfactory is positive, where the criteria are met;*
- *Deficient is negative, where the criteria are not met;*
- *Alternative Control is neutral, where another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and*
- *N/A is neutral, where the control, or AO, does not apply.*

3PAAC Standard 6.6: Objectivity Through Reasonable Interpretation

SCF Assessors must maintain objectivity through the following:

(1) **Reasonable interpretation of:**
   a. **Controls; and**
   b. **When available, AOs; and**

(2) **Analysis of relevant evidence from:**
   a. **Examinations;**
   b. **Interviews; and/or**
   c. **Testing.**

Justification: Assessors operate from a position of trust and authority. Therefore, assessors must utilize objectivity through reasonable interpretation of both AOs and evidence. Objectivity and reasonableness are cornerstone expectations for any professional. The testing of controls determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the applicable AOs.

Guidance: If a control doesn't meet the intent of the design, there is no need to test its effectiveness. Assessors should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on:[64]

- *Review techniques:*
  - *Documentation review;*
  - *Log review;*
  - *Ruleset review;*
  - *System configuration review;*

[64] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

- *Network sniffing and;*
- *File integrity checking; and*

- *Target identification and analysis techniques:*
  - *Network discovery;*
  - *Network port and service identification;*
  - *Vulnerability scanning; and*
  - *Wireless scanning.*

Appendix D: Adequate Security provides context about determining "reasonableness" in the context of evaluating cybersecurity and/or data protection controls. For a SCF 3PAO to maintain reasonable interpretation by its assessment team, it is expected to:

- *Implement sound hiring practices to attract and retain quality individuals;*
- *Ensure assessors receive continuing education that is specific to assessment-related activities to maintain situational awareness of leading industry practices; and*
- *Perform After Action Reviews (AARs) with an OSA to identify possible conflicts where reasonable interpretation was not followed.*

3PAAC Standard 6.7: Adequate Sampling

For reasonable evidence of conformity:

(1) SCF Assessors must obtain an adequate sampling of applicable evidence to make a reasonable determination of conformity; and

(2) The sampling must represent the period of operation relevant to the assessment.

Justification: Assessors are expected to use one (1), or more, of these sampling methods to help ensure that the assessment results are representative of the overall environment, providing a reliable basis for evaluating control effectiveness:

- *Simple random sampling;*
- *Stratified sampling;*
- *Systemic sampling; and/or*
- *Cluster sampling.*

Guidance: Simple random sampling is preferred for performing 3PAAC Standard and Enhanced assessments. This involves randomly selecting a subset of people, processes, technologies, data sets and facilities to evaluate cybersecurity and/or data protection controls.

Appendix D: Adequate Security provides context about determining adequacy. The assessor establishes adequate evidence to support a conclusion of sufficient operation for the period as follows:

- *Adequate evidence is defined by reasonable, not absolute assurance principles; and*
- *Adequacy is determined by the assessor for each control included in the scope boundary.*

Adequate evidence of conformity would suggest multiple samples are selected across the previous twelve (12)-month period of operation in which the samples would be available and in the same format for a randomized period of dates selected by the assessor, validating the evidence (e.g., log file) was present and generated for that period (e.g., asset created the log event).

3PAAC Standard 6.8: Assessment Tools & Automation

SCF 3PAOs must implement assessment-related mechanisms to:

(1) Improve accuracy; and

(2) Reduce human error.

Justification: Traditional, manual assessment methodologies are inefficient and error-prone. SCF 3PAOs should incorporate automated mechanisms (e.g., a Governance, Risk & Compliance (GRC) solution) or advanced assessment tools (e.g., Artificial Intelligence and Autonomous Technologies (AAT)) to:

- *Increase the efficiency of the assessment process; and*
- *Reduce:*
  - *Human error; and*

- *The ability of an assessor to skew data.*

Guidance: Relying on hand-written notes or ad hoc spreadsheets is something that SCF 3PAOs should strive to avoid. The use of Governance, Risk & Compliance (GRC) platforms with specific control assessment functions should be considered a minimal expectation for an assessment tool utilized by SCF 3PAO for 3PAAC Services.

3PAAC Standard 7: Quality Control

SCF 3PAOs must systematically examine and evaluate assessment processes, procedures, activities and deliverables to ensure compliance with established quality standards and requirements.

Justification: An assessment's results can have positive, negative or neutral consequences for the OSA. Therefore, quality control by the SCF 3PAO is crucial to ensure the assessment results accurately reflect the actual state of cybersecurity and/or data protection controls. This requires internal quality control processes by the SCF 3PAO.

Guidance: The SCF 3PAO is expected to adhere to a relevant Quality Management System (QMS), as defined by industry-recognized practices (e.g., ISO 9001, ISO 17020, etc.).

3PAAC Standard 7.1: Assessment Findings

To ensure the ability of a reasonable individual, having a similar amount of knowledge and experience, to arrive at the same conclusion(s), SCF 3PAOs must:

(1) Document assessment findings;
(2) Objectively confirm the validity of the assessment team's conclusions; and
(3) If applicable, submit assessment results to the appropriate:
  a. Accreditation Body (AB); or
  b. Governing body.

Justification: Assessment teams may be made up of both employees of a SCF 3PAO and independent contractors. Due to this possible transitory nature of individual assessors, assessment findings must be documented in a manner that a reasonable individual, with similar qualifications and experience, could evaluate the same facts and circumstances and arrive at the same conclusion as the original assessor.

Guidance: The documentation of assessment findings to ensure reasonableness is expected to be included in the SCF 3PAO's quality control processes. The documentation of assessment findings should include but is not limited to:

- *Detailed descriptions of the findings and their impact on the OSA's cybersecurity posture;*
- *Evidence supporting each finding, such as logs, screenshots, or interview notes; and*
- *Recommendations for remediation and timelines for implementing corrective actions.*

Assessors may provide initial findings to the OSA as "end of day" or "end of period" out briefing to give the OSA situational awareness on the status of the assessment.

SCF 3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment related:[65]

- *Mitigating recommendations;*
- *Reporting; and*
- *Remediation/mitigation.*

3PAAC Standard 7.2: Objective Peer Review

SCF Assessors must obtain an objective peer review of all assessment-related findings before presenting findings to the OSA.

[65] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

Justification: Objectivity is essential when documenting assessment findings. Reviewing the findings by a qualified, competent individual not part of the assessment team is crucial to produce a quality assessment report. Internal peer reviews ensure objectivity by having assessment findings evaluated by someone independent of the assessment process. This practice helps identify potential biases or errors and ensures that findings are based on evidence and aligned with established criteria.

Guidance: Peer reviews by people other than the assessment team are expected to be part of the SCF 3PAO's quality control processes. Peer reviews can be from an internal or third-party resource.

3PAAC Standard 8: Conformity Designation

SCF 3PAOs must summarize assessment results with a conformity designation. Only one (1) of the following four (4) possible conformity designations may be used:

(1) STRICTLY CONFORMS. The designation of Strictly Conforms is a positive outcome. Strictly Conforms indicates:

- **a. The OSA can demonstrate Strict Conformity with its selected cybersecurity and/or data protection controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:**
  - **i. The controls are met and operational;**
  - **ii. Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or**
  - **iii. Where applicable, compensating controls are validated by the assessor as being:**
    1. **Applicable;**
    2. **Reasonable; and**
    3. **Implemented and operating properly; and**
- **b. Assessed controls provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:**
  - **i. Adheres to a defined and documented risk tolerance;**
  - **ii. Mitigates material cybersecurity and/or data protection risks;**
  - **iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and**
  - **iv. Is prepared to respond to material incidents.**

(2) CONFORMS. The designation of Conforms is a positive outcome. Conforms indicates:

- **a. The OSA can demonstrate conformity with its selected cybersecurity and/or data protection controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:**
  - **i. The controls are met and operational;**
  - **ii. Any control designated as N/A is validated as such by the assessor; and/or**
  - **iii. Where applicable, compensating controls are validated by the assessor as being:**
    1. **Applicable;**
    2. **Reasonable; and**
    3. **Implemented and operating properly;**
- **b. Any assessed control deficiency is not material to the OSA's cybersecurity and data protection program; and**
- **c. Assessed controls provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:**
  - **i. Adheres to a defined and documented risk tolerance;**
  - **ii. Mitigates material cybersecurity and/or data protection risks;**
  - **iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and**
  - **iv. Is prepared to respond to material incidents.**

(3) SIGNIFICANT DEFICIENCY. The designation of Significant Deficiency is a negative outcome. Significant Deficiency indicates:

- **a. The OSA can demonstrate limited conformity with its selected cybersecurity and/or data protection controls due to a systemic problem within the OSA's cybersecurity and data protection program, where:**
  - **i. At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:**
    1. **The controls are met and operational;**
    2. **Any control designated as N/A is validated as such by the assessor; and/or**
    3. **Where applicable, compensating controls are validated by the assessor as being:**
       a. **Applicable;**

        b. Reasonable; and
        c. Implemented and operating properly;
    b. Any assessed control deficiency is not material to the OSA's cybersecurity and data protection program;
    c. Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:
        i. Adheres to a defined and documented risk tolerance;
        ii. Mitigates material cybersecurity and/or data protection risks;
        iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
        iv. Is prepared to respond to material incidents; and
    d. The OSA's cybersecurity and data protection program:
        i. Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
        ii. Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data protection controls.

(4) MATERIAL WEAKNESS. The designation of Material Weakness is a negative outcome. Material Weakness indicates:
    a. The OSA cannot demonstrate conformity with its selected cybersecurity and/or data protection controls due to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:
        i. One (1), or more, material controls is/are deficient; and/or
        ii. Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
            1. The controls are met and operational;
            2. Any control designated as N/A is validated by the assessor and confirmed as such; and/or
            3. Where applicable, compensating controls are validated by the assessor as being:
                a. Applicable;
                b. Reasonable; and
                c. Implemented and operating properly;
    b. Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data protection program adequately:
        i. Adheres to a defined and documented risk tolerance;
        ii. Mitigates material cybersecurity and/or data protection risks; and/or
        iii. Possesses the capability to:
            1. Detect and protect against material cybersecurity and/or data protection threats; and/or
            2. Respond to material incidents; and
    c. The OSA's cybersecurity and data protection program:
        i. Cannot perform its stated mission; and
        ii. Drastic changes to people, processes and/or technologies are required to remediate the deficiencies.

Justification: A systemic weakness across existing assessment methodologies is the lack of a standardized assessment conformity designation. Assessment conformity designations are supported by 3PAAC Standard 6.5 (Control Designation) and are used to summarize the overall assessment.

Guidance: See Appendix D: Adequate Security for more details on defining adequate security. The assessment conformity designation is intended for the OSA's executive leadership team to clearly and unambiguously provide a "pass or fail score" to the assessment. The use of the terminology in this standard is recognized throughout the industry, so it avoids reinventing the concept.

An OSA cannot have a Strictly Conforms, Conformity or Significant Deficiency designation with a Material Weakness determination in one (1), or multiple, domain(s)/family(ies) of cybersecurity and/or data protection controls included in the assessment boundary.

3PAAC Standard 8.1: Report On Conformity (ROC)

SCF 3PAOs must produce a written Report on Conformity (ROC) that uses persuasive, reasonable evidence to defend the assessment conformity designation.

Justification: The assessment results must be documented in a professional format capable of defending the assessment conformity designation.

Guidance: The format of a ROC is not standardized in the industry and would be up to a governing body, or SCF 3PAO, to define its specific needs. A ROC should include, but is not limited to the following elements:

- *Disclosure of the level of rigor selected for 3PAAC Services (see Appendix C for details on Assessment Rigor);*
- *A summary of the assessment scope and objectives;*
- *Detailed findings and evidence supporting each determination;*
- *An executive summary highlighting the overall conformity status (e.g., Strictly Conforms, Conforms, Significant Deficiency, Material Weakness);*
- *Recommendations for remediation where deficiencies are identified; and*
- *A section for the OSA to respond to findings or submit challenges.*

This format ensures that the ROC is comprehensive and provides all necessary information for stakeholders to understand the assessment results.

SCF 3PAOs are expected to link persuasive, reasonable evidence to the applicable level of rigor and available evidence.

3PAAC Standard 8.2: Assessment Finding Challenges

SCF 3PAOs must have a formal process to:

(1) Intake, review and respond to an OSA's challenges regarding assessment findings, as defined in the:
- **a. MSA; and/or**
- **b. SOW; and**

(2) Settle challenges through:
- **a. Direct negotiation;**
- **b. If applicable, the applicable Accreditation Body (AB);**
- **c. Arbitration; or**
- **d. The applicable legal venue, as defined in the:**
  - **i. MSA; and/or**
  - **ii. SOW.**

Justification: SCF 3PAOs and OSAs have the right to disagree. However, the ROC reflects the point-in-time observations of the SCF 3PAO's assessment team. These assessment findings affect the assessment conformity designation issued by the SCF 3PAO. Therefore, SCF 3PAOs must be prepared to handle challenges to assessment findings professionally and responsively. It is reasonable to expect that assessment conformity designation, particularly those identifying a Significant Deficiency or Material Weakness, may lead to disputes or challenges from the OSA. A formalized process for handling these challenges is necessary to maintain the integrity of the assessment and ensure that all concerns are addressed in a fair and transparent manner. This process should include clear guidelines for submitting challenges, timelines for review, criteria for evaluating challenges and procedures for resolution.

Guidance: The SCF 3PAO must ensure the SOW and other documentation it uses as part of its 3PAAC Services covers the processes around challenging assessment findings. This may require legal arbitration for points of contention that cannot be settled solely by the SCF 3PAO and OSA.

To help eliminate unexpected results, assessors may provide initial findings to the OSA as "end of day" or "end of period" out briefing to give the OSA situational awareness on the status of the assessment.

3PAAC Standard 9: Maintaining Conformity

OSA must seek re-assessment when there is a material change to the assets and/or processes that make up the assessment boundary. Changes are defined as:

(1) **Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.**

(2) **Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.**

Justification: A SCF 3PAO-issued attestation and/or certification is voided when material changes affect the assessment boundary, since the basis for the attestation and/or certification is no longer applicable.

Guidance: The timeline for remediation should be agreed upon between the SCF 3PAO and the OSA, since the timeline is dependent upon the risk appetite of the organization. However, unless justified by a legitimate business, or technical, reason no POA&M item should be older than one-hundred eighty (180) days. Items older than that should be considered deficient.

- *Assessor has the ability to re-evaluate controls during the course of the assessment and for up to ten (10) business days following the active assessment period.*
- *A "plan to address" a deficiency does not suffice as evidence to support control conformity. The plan to remediate a deficiency must be implemented and operational.*

An OSA's material changes to any certified environment should be coordinated with the SCF 3PAO that performed the most recent assessment. That SCF 3PAO should be contracted to conduct 3PAAC Services to validate, or re-issue, an attestation and/or certification.

- *Material changes have a strategic and/or operational impact on the OSA's cybersecurity and/or data protection capabilities; and*
- *Non-material changes have a tactical-focused impact on the OSA's cybersecurity and/or data protection capabilities.*

3PAAC Standard 9.1: Plan of Action & Milestones (POA&M)

OSA must document control deficiencies in a Plan of Action & Milestones (POA&M), or similar form of control deficiency tracking mechanism, at a minimum identifies the following:

(1) **Deficient control(s);**
(2) **A description of the control deficiency(ies);**
(3) **Affected people, processes, technologies, data and/or facilities;**
(4) **Designated Point of Contact (POC) for remediation efforts;**
(5) **Remediation plan (e.g., milestones, resources needed, etc.);**
(6) **Scheduled remediation date; and**
(7) **Date remediation was completed.**

Justification: A formal methodology is necessary to document identified tasks, responsibilities and milestones associated with control deficiencies. It provides a clear roadmap for addressing weaknesses, assigns responsibilities and sets deadlines for completion, ensuring accountability and timely resolution.

Guidance: The timeline for remediation should be agreed upon between the SCF 3PAO and the OSA, since the timeline is dependent upon the risk appetite of the organization. However, unless justified by a legitimate business, or technical, reason no POA&M item should be older than one-hundred eighty (180) days. Items older than that should be considered deficient.

- *Assessor has the ability to re-evaluate controls during the course of the assessment and for up to ten (10) business days following the active assessment period.*
- *A "plan to address" a deficiency does not suffice as evidence to support control conformity. The plan to remediate a deficiency must be implemented and operational.*

A POA&M is a "living document" that can exist in a manner that works best for the OSA, ranging from a simple Excel spreadsheet that serves as a risk register or it can be a dedicated module in a GRC technology platform. POA&Ms:

- *Identify tasks that need to be accomplished;*
- *Provides details on resources required to achieve the elements of the plan;*
- *Target milestones to meeting the tasks; and*
- *Track remediation efforts and dates for those milestones.*

3PAAC Standard 9.2: Changes Affecting The Assessment Boundary

A SCF 3PAO-issued attestation and/or certification is invalidated following any material change to the assets and/or processes that make up the OSA's assessment boundary.

Justification: A SCF 3PAO-issued attestation and/or certification is voided when material changes affect the assessment boundary. Only through a reassessment of the changes can a certification be maintained. Reassessing the environment after any material change is crucial because such changes can significantly alter the risk landscape and the effectiveness of existing controls.

Guidance: Proper change management practices must consider the implications of making proposed changes. Therefore, material changes should be coordinated with a SCF 3PAO, where an internal audit should be performed once the changes are implemented and then followed by a SCF 3PAO to conduct 3PAAC Services to validate, or re-issue, an attestation and/or certification.

For example, if a company implements a new data management system or undergoes a significant restructuring, these changes could introduce new vulnerabilities or affect the applicability of current controls. To maintain the validity of an attestation, or certification, a reassessment ensures that all controls remain effective and that the organization continues to meet its cybersecurity and data protection obligations.

3PAAC Standard 9.3: Reassessments Due To Material Change

As part of a reassessment due to material change, SCF Assessors:

(1) Must:

a. Conduct 3PAAC Services consistent with the original assessment's rigor on the assets and/or processes affected by a material change; and

b. Limit the scope of the reassessment to the assets and/or processes that changed; and

(2) May rely on the findings from the most recent, current assessment for unaffected assets and/or processes.

Justification: Engaging a SCF 3PAO to perform a limited assessment for material changes is intended to make 3PAAC Services sustainable from a cost and labor perspective. Conducting a targeted reassessment after material changes ensures that the assessment scope is focused on areas impacted by the changes, optimizing the use of resources and minimizing costs.

Guidance: Per 3PAAC Standard 9, material and non-material changes are defined as:

- *Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.*
- *Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.*

A new assessment is required if there are significant architectural or boundary changes to the previous assessment scope. Examples include, but are not limited to:

- *Expansions of networks;*
- *Mergers and Acquisitions (M&A) activities;*
- *Operational changes within assessment boundary(ies) such as new or changed:*
  - *Technology platforms (e.g., OS migration from Windows to Linux);*
  - *ESP integrations; and/or*
  - *Facilities.*

To effectively coordinate reassessments, an OSA should:

- *Conduct pre-change consultation. The OSA should consult with the SCF 3PAO before implementing significant changes to understand potential impacts;*
- *Conduct an internal audit. Once changes are implemented, the OSA should conduct an internal audit to identify any immediate issues or risks introduced by the changes; and*
- *Engage a SCF 3PAO to schedule a reassessment. Based on the internal audit findings, the OSA should engage the SCF 3PAO to perform a targeted reassessment that focuses solely on the affected areas.*

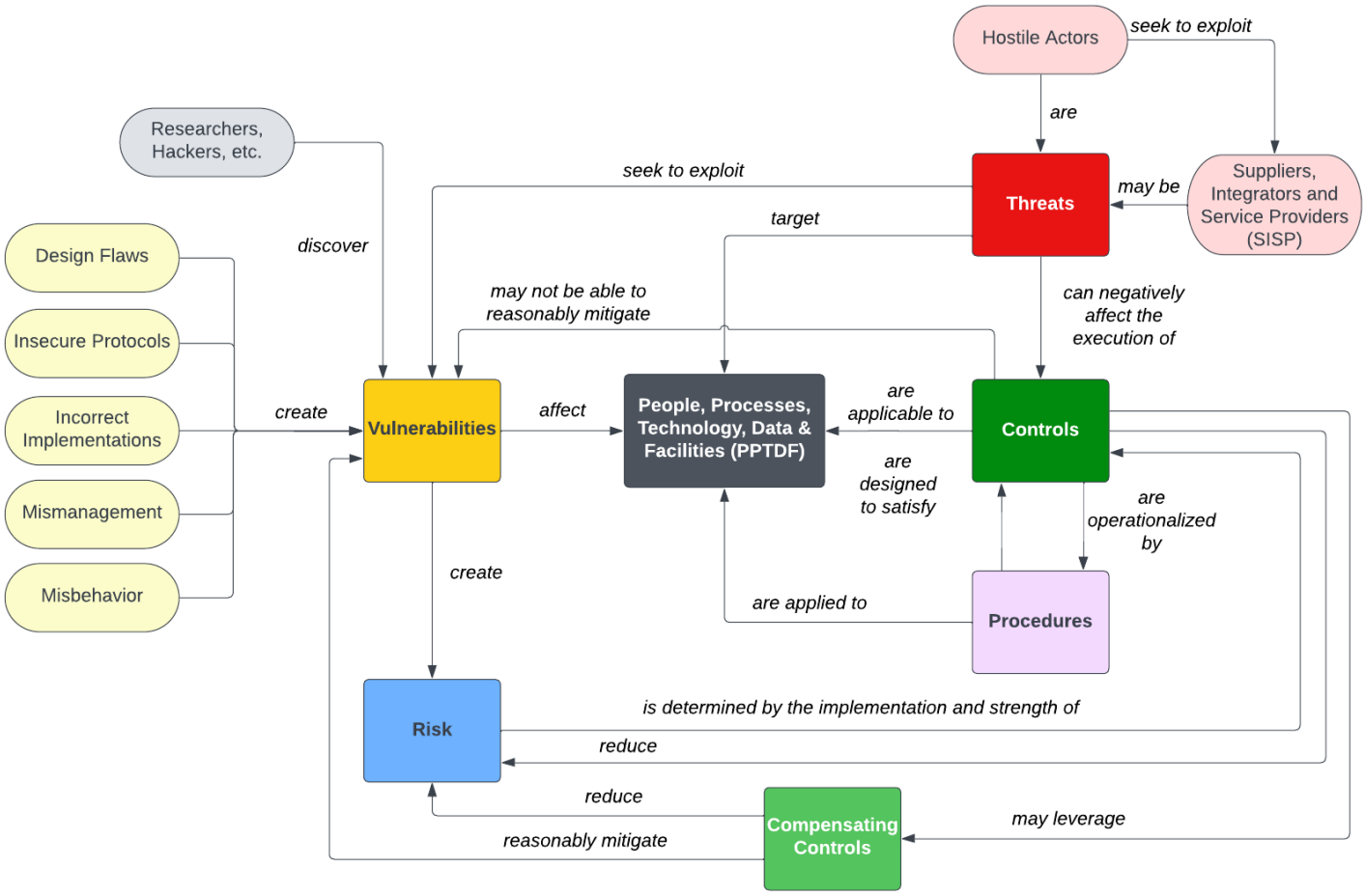
ERRATA

Version 1.0 – Initial publication.

APPENDICES

APPENDIX A: RISK TERMINOLOGY NORMALIZATION

Threat, vulnerability and risk management practices are meant to achieve a minimum level of protection - this equates to a reduction in the total risk due to the protections offered by implemented controls. These ecosystem components have unique meanings that need to be understood to reasonably protect people, processes, technology and data. Understanding the context of how these components integrate can lead to more meaningful and practical risk management practices.



As it pertains to the CDPAS:

- Risk Appetite: *the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.*[66]
- Risk Tolerance: *the level of risk an entity is willing to assume in order to achieve a potential desired result.* [67]
- Risk Threshold: *values used to establish concrete decision points and operational control limits to trigger management action and response escalation.*[68]

RISK APPETITE

A risk appetite is a broad "risk management concept" used to inform employees about what is and is not acceptable, regarding risk management from an organization's executive leadership team. A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective. Similar in concept to how a policy is a *"high-level*

[66] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[67] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[68] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

statement of management intent," an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted. [69]

Examples of an organization stating its risk appetite from basic to more complex statements:

- *"[organization name] is a low-risk organization and will avoid any activities that could harm its customers."*
- *"[organization name] will aggressively pursue innovative solutions through Research & Development (R&D) to provide industry-leading products and services to our clients, while maintaining a Moderate Risk Appetite. Developing breakthrough products and services does invite potential risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Proposed business practices that pose greater than a Moderate Risk will be considered on a case-by-case basis for financial, operational and legal implications."*

It is important to point out that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they issue risk appetite statements, but the Business As Usual (BAU) practices routinely violate the risk appetite. This is often due to numerous reasons that include, but are not limited to:

- Technical debt;
- Dysfunctional management decisions;
- Insecure practices;
- Inadequate funding/resourcing;
- Improperly scoped support contracts (e.g., Managed Service Providers (MSPs), consultants, vendors, etc.); and
- Lack of pre-production security testing.

Risk Tolerance

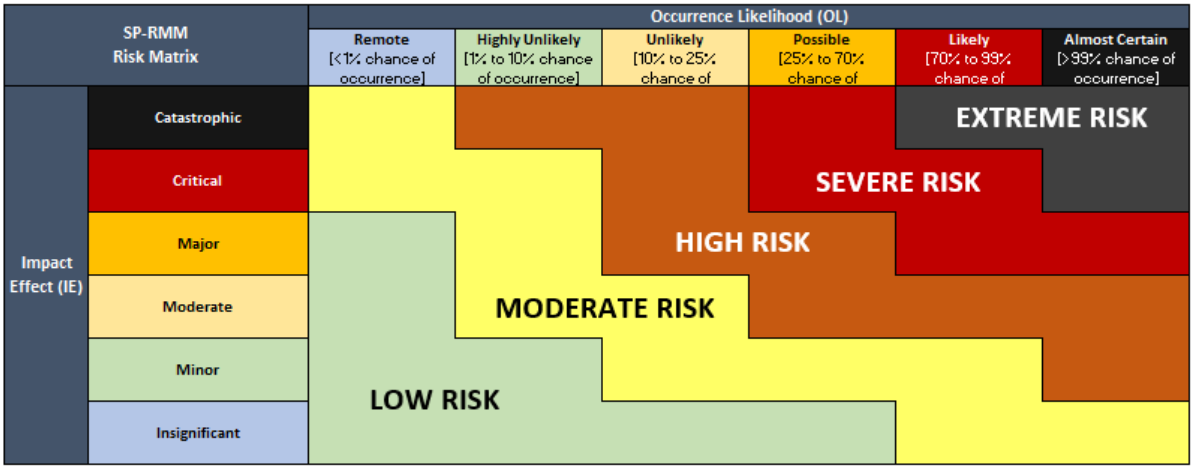
Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of risk enables risk assessments to leverage those same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

(1) Low Risk;
(2) Moderate Risk;
(3) High Risk;
(4) Severe Risk; and
(5) Extreme Risk.

There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

(1) Impact Effect (IE); and
(2) Occurrence Likelihood (OL).



[69] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf*

The six (6) categories of IE are:

(1) Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
(2) Minor *(e.g., organization-defined minor impacts to business operations)*;
(3) Moderate *(e.g., organization-defined moderate impacts to business operations)*;
(4) Major *(e.g., organization-defined major impacts to business operations)*;
(5) Critical *(e.g., organization-defined critical impacts to business operations)*; and
(6) Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

The six (6) categories of OL are:

(1) Remote possibility *(e.g., <1% chance of occurrence)*;
(2) Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
(3) Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
(4) Possible *(e.g., from 25% to 70% chance of occurrence)*;
(5) Likely *(e.g., from 70% to 99% chance of occurrence)*; and
(6) Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches commonly employed to estimate OL:

(1) Relevant historical data;
(2) Probability forecasts; and
(3) Expert opinion.

An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices).
- Organization-specific threats (natural and manmade).
- Reasonably expected industry practices.
- Pressure from competition.
- Executive management decisions.

Low Risk Tolerance

Organizations that may adopt a Low Risk Tolerance include, but are not limited to, those that:

- Provide products and/or services that are necessary for the population to maintain normalcy in daily life;
- Exist in a highly regulated industry with explicit cybersecurity and/or data protection requirements;
- Store, process and/or transmit highly sensitive/regulated data;
- May be a legitimate target for nation-state actors to disrupt and/or compromise due to the high-value nature of the organization;
- Have strong executive management support for cybersecurity and data protection practices as part of “business as usual” activities;
- Maintain a high level of capability maturity for preventative cybersecurity controls to implement “defense in depth” protections across the enterprise;
- Have a high level of situational awareness (cybersecurity & physical) that includes its supply chain; and
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Low Risk Tolerance include, but are not limited to:

- Critical infrastructure;
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.);
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, Cloud Service Providers (CSPs), etc.) (high value);
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.);
- Technology Research & Development (R&D) (high value);
- Healthcare (high value); and
- Government institutions:
    - Military;
    - Law enforcement;
    - Judicial system;

- Financial services (high value); and
- Defense Industrial Base (DIB) contractors (high value).

Moderate Risk Tolerance

Organizations that may adopt a Moderate Risk Tolerance include, but are not limited to, those that:

- Exist in a regulated industry that has specific cybersecurity and/or data protection requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.);
- Store, process and/or transmit sensitive/regulated data;
- Have "flow down" requirements from customers that require adherence to certain cybersecurity and/or data protection requirements;
- Have executive management support for initiatives to secure sensitive / regulated data enclaves;
- May be a legitimate target for attackers who wish to financially benefit from stolen information or ransom; and
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Moderate Risk Tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.);
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.);
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, etc.);
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.);
- Technology services (e.g., Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), etc.);
- Manufacturing (high value);
- Healthcare;
- Defense Industrial Base (DIB) contractors and subcontractors;
- Legal services (e.g., law firms); and
- Construction (high value).

High Risk Tolerance

Organizations that may adopt a High Risk Tolerance include, but are not limited to, those that:

- Exist in an unregulated industry, pertaining to expected cybersecurity and/or data protection practices;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity and data protection governance practices; and
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups;
- Hospitality industry (e.g., restaurants, hotels, etc.);
- Construction;
- Manufacturing; and
- Personal services.

Severe Risk Tolerance

Organizations that may adopt a Severe Risk Tolerance include, but are not limited to, those that:

- Exist in an unregulated industry, pertaining to expected cybersecurity and/or data protection practices;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity and data protection governance practices; and
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a Severe Risk Tolerance include, but are not limited to:

- Startups; and
- Artificial Intelligence (AI) developers.

Extreme Risk Tolerance

Organizations that may adopt an Extreme Risk Tolerance include, but are not limited to, those that:

- Exist in an unregulated industry, pertaining to expected cybersecurity and/or data protection practices;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity and data protection governance practices; and

- Do not have cyber-related liability insurance.

Organizations that may choose to operate with an Extreme Risk Tolerance include, but are not limited to:

- Startups; and
- AI developers.

Risk Thresholds

Risk thresholds are directly tied to risk tolerance and utilize organization-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the different levels of risk tolerance (e.g., Low, Moderate and High Risk). By establishing these risk thresholds, it provides a means of comparing relative risk to an organization. Risk thresholds are criteria that are unique to an organization such as organization-specific activities / scenarios that could:

- Damage the organization's reputation;
- Negatively affect short-term and long-term profitability; and/or
- Impede business operations.

Risk thresholds are entirely unique to each organization, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

APPENDIX B: ASSESSMENT RIGOR

The SCF CAP assessment rigor is based on assessment methods described in NIST SP 800-172A Appendix C.[70] There are three (3) levels of rigor:

(1) Standard;
(2) Enhanced; and
(3) Comprehensive.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

LEVEL 1 RIGOR: STANDARD

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

(1) Implemented; and
(2) Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

(1) Is relevant to a specific point in time (time at which the controls were evaluated); and
(2) Relies on the manual review of artifacts to derive a finding.

<table>
<tr><th colspan="2">STANDARD
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
▪ Security safeguard existence;
▪ Functionality;
▪ Correctness;
▪ Completeness; and
▪ Potential for improvement over time.

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:
(1) Implemented; and
(2) Free of obvious errors.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections of the assessment object.

This type of examination is conducted using a limited</td><td>An interview that consists of broad-based, high-level discussions with individuals or groups of individuals.

This type of interview is conducted using a set of</td><td>A test methodology assumes no knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “black box” testing.</td></tr>
</table>

[70] *NIST SP 800-172A - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf*

		body of evidence or documentation including: ▪ Functional-level descriptions for mechanisms; ▪ High-level process descriptions for activities; and ▪ Documents for specifications.	generalized, high-level questions.	This type of testing is conducted using: ▪ A functional specification for mechanisms; and A high-level process description for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 2 RIGOR: ENHANCED

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

(1) The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
(2) There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

(1) Is relevant to a specific point in time (time at which the controls were evaluated);
(2) In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
(3) The combined output of automated and manual reviews of artifacts is used to derive a finding.

<table>
<tr><th colspan="2">ENHANCED
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
(1) The applicable controls are:
a. Implemented; and
b. Free of obvious/apparent errors; and
(2) There are increased grounds for confidence that the applicable controls are:
a. Implemented correctly; and
b. Operating as intended.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections and more in-depth studies and analyses of the assessment object. This type of examination is conducted using a substantial body of evidence or documentation.

Examples include:
Functional-level descriptions and where appropriate and available, high-level design</td><td>An interview that consists of broad-based, high-level discussions and more in-depth discussions in specific areas with individuals or groups of individuals.

This type of interview is conducted using:
A set of generalized, high-level questions; and
More in-depth questions in specific areas where responses indicate a need for more in-depth investigation.</td><td>A test methodology assumes some knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “gray box” testing.

This type of testing is conducted using:
A functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-</td></tr>
</table>

		information for mechanisms; ▪ High-level process descriptions and implementation procedures for activities; and ▪ Documents and related documents for specifications.		level process description; and ▪ A high-level description of integration into the operational environment for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 3 RIGOR: COMPREHENSIVE

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

(1) Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
(2) Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and
(3) There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

(1) AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
(2) Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

<table>
<tr><th colspan="2">COMPREHENSIVE
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:
(1) Whether the applicable controls are:
a. Implemented; and
b. Free of obvious/apparent errors;
(2) Whether there are further increased grounds for confidence that the applicable controls are:
a. Implemented correctly; and
b. Operating as intended on an ongoing and consistent basis; and
(3) There is support for continuous improvement in the effectiveness of the applicable controls.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections and more in-depth, detailed and thorough studies and analyses of the assessment object.

This type of examination is conducted using an extensive</td><td>An interview that consists of broad-based, high-level discussions and more in-depth, probing discussions in specific areas with individuals or groups of individuals.

This type of interview is conducted using:</td><td>Test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “white box” testing.</td></tr>
</table>

		body of evidence or documentation including:
		▪ Functional-level descriptions and where appropriate and available:
		  ○ High- level design information;
		  ○ Low-level design information; and
		  ○ Implementation information for mechanisms;
		▪ High-level process descriptions and detailed implementation procedures for activities; and
		▪ Documents and related documents for specifications.
			▪ A set of generalized, high-level questions; and
			▪ More in-depth, probing questions in specific areas where responses indicate a need for more in-depth investigation.
				This type of testing is conducted using:
				▪ A functional specification;
				▪ Extensive system architectural information (e.g., high-level design, low-level design);
				▪ Implementation representation (e.g., source code, schematics) for mechanisms;
				▪ A high-level process description; and
				▪ A detailed description of integration into the operational environment for activities.

	Breadth of Coverage	Examinations uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
		▪ Whether the applicable controls are:
		  ○ Implemented; and
		  ○ Free of obvious/apparent errors;
		▪ Whether there are further increased grounds for confidence that the applicable controls are:
		  ○ Implemented correctly; and
		  ○ Operating as intended on an ongoing and consistent basis; and
		▪ There is support for continuous improvement in the effectiveness of the applicable controls.
			Interviews use a sufficiently large sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
			▪ Whether the applicable controls are:
			  ○ Implemented; and
			  ○ Free of obvious/apparent errors;
			▪ Whether there are further increased grounds for confidence that the applicable controls are:
			  ○ Implemented correctly; and
			  ○ Operating as intended on an ongoing and consistent basis; and
			▪ There is support for continuous improvement in the effectiveness of the applicable controls.
				Testing uses a sufficiently large sample of assessment objects by type and number within type and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
				▪ Whether the applicable controls are:
				  ○ Implemented; and
				  ○ Free of obvious/apparent errors;
				▪ Whether there are further increased grounds for confidence that the applicable controls are:
				  ○ Implemented correctly; and
				  ○ Operating as intended on an ongoing and consistent basis; and
				▪ There is support for continuous improvement in the effectiveness of the applicable controls.

Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.

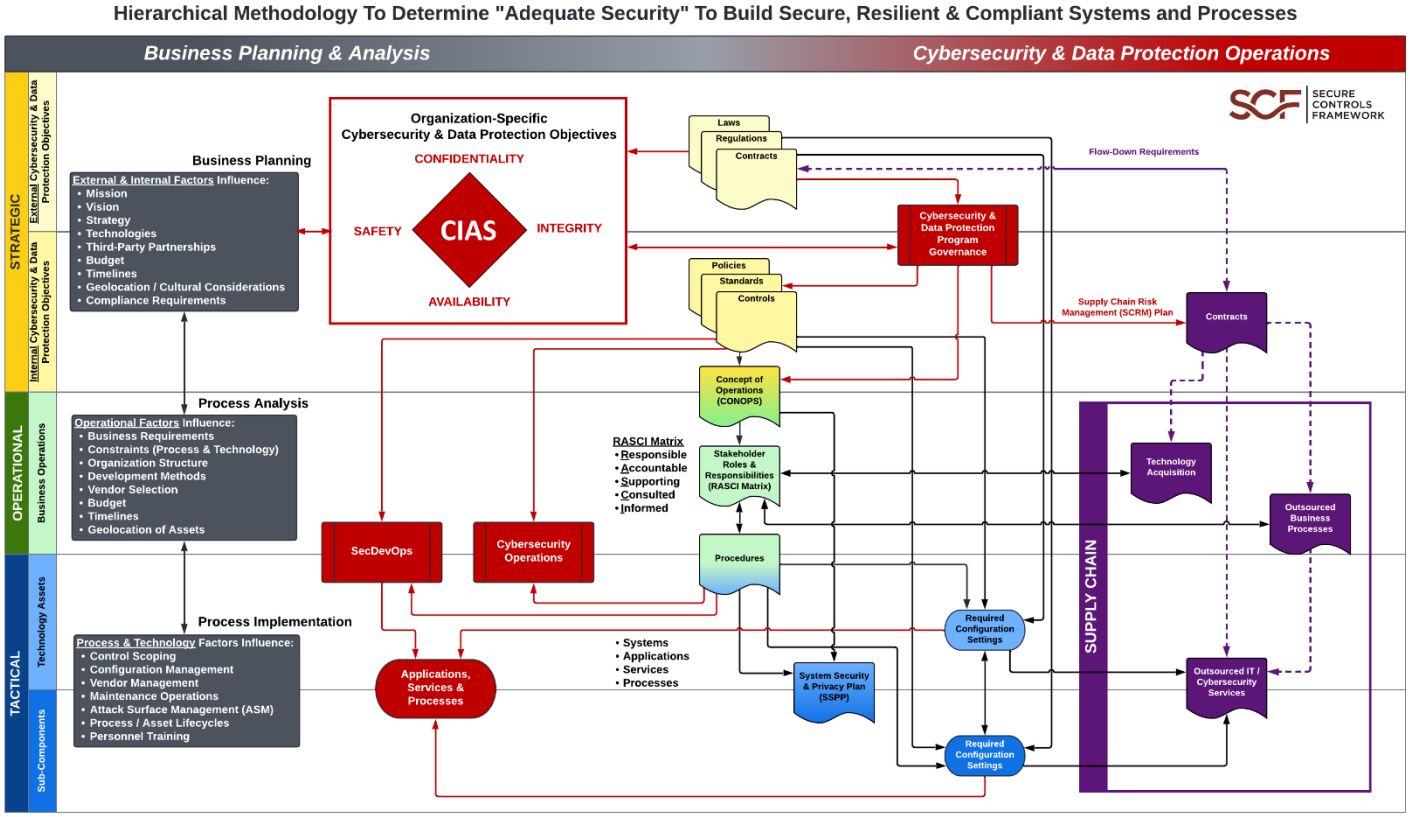
		▪ Firmware.		
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	N/A

APPENDIX C: ADEQUATE SECURITY

The SCF CAP recognizes that no technology can provide "absolute security" due to the limits of human certainty. This uncertainty exists in the lifecycle of every system, application and/or product and is often due to the constraints of cost, schedule, performance, feasibility and practicality. Therefore, trade-offs must be routinely made across contradictory, competing and conflicting needs and limitations. However, these trade-offs must be optimized to achieve "adequate security," reflecting a risk-based decision by stakeholders. [71]

The SCF CAP, through the CDPAS, leverages concepts from NIST SP 800-160 to explain the holistic concepts of how broader business planning and analysis ultimately lead to actionable cybersecurity and/or data protection requirements. Understanding this hierarchical nature of requirements is a fundamental construct of cybersecurity and/or data protection control governance processes.

This concept is depicted in the following graphic for how the concept of adequate security is based on business planning and analysis as it relates to establishing protection requirements: [72]



An organization publishes policies to eliminate potential gaps in that desired governed behavior to achieve "adequate security" based on what a reasonable individual would be expected to do in a similar situation. The rules associated with this "governed behavior" must be accurate, consistent, compatible and complete with respect to the executive leadership's objectives to accomplish the organization's mission and overall strategy.

An organization's policies ultimately define the behavior of Individual Contributors (IC) (e.g., engineers, analysts, developers, etc.) in performing their roles and associated responsibilities for developing processes and procedures. This eventually leads to the configuration of technology assets (e.g., systems, applications, services and processes), where a discrete set of restrictions and properties must exist to specify how that asset enforces or contributes to implementing organizational security policies.

[71] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*
[72] *SCF Adequate Security Determination Process - https://securecontrolsframework.com/content/adequate-cybersecurity-methodology.pdf*

The required configuration settings for technology assets must include technical and business requirements, which ultimately fall under organizational cybersecurity and/or data protection policies. Requirements can be categorized as follows: [73]

- Stakeholder requirements that address the need to be satisfied in a design-independent manner; and
- System requirements express the specific solution that will be delivered in a design-dependent manner.

Establishing Secure Systems

A "secure system" is a system that ensures that only the authorized intended behaviors and outcomes occur, thereby providing freedom from those conditions, both intentionally/with malice and unintentionally/without malice, that can cause a loss of information assets with unacceptable consequences.[74] This definition expresses an ideal that captures three (3) essential aspects of what it means to achieve security:

(1) Enable the delivery of the required system capability despite intentional and unintentional forms of adversity;
(2) Enforce constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized while satisfying the first aspect; and
(3) Enforce constraints based on rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur, while satisfying the second aspect.

For a system, adequate security is an evidence-based determination that achieves and optimizes security performance against all other performance objectives and constraints. Judgments of adequate security are driven by the stakeholder objectives, needs and concerns associated with the system. Adequate security has two elements:

- Achieve the minimum acceptable threshold of security performance; and
- Maximize security performance to the extent that any additional increase in security performance degrades some other aspects of system performance or requires an unacceptable operational commitment.

Defining Stakeholder Security Requirements

Stakeholder security requirements are those stakeholder requirements that are security-relevant. Stakeholder security requirements specify:

- The protection needed for the mission or business, data, information, processes, functions, human and system assets;
- The roles, responsibilities and security-relevant actions of individuals who perform and support the mission or business processes;
- The interactions between the security-relevant solution elements; and
- The assurance that is to be obtained in the security solution.

Defining System Security Requirements

System requirements specify the technical view of a system or solution that meets the identified stakeholder needs. The system requirements are a transformation of the validated stakeholder requirements. System requirements specify what the system or solution must do to satisfy the stakeholder requirements. System security requirements are those system requirements that are security relevant. These requirements define:

- The protection capabilities provided by the security solution;
- The performance and behavioral characteristics exhibited by the security solution;
- Assurance processes, procedures and techniques;
- Constraints on the system and the processes, methods and tools used to realize the system; and
- The evidence required to determine the system security requirements have been satisfied.

System of Systems Mindset

A system is *"an arrangement of parts or elements that together exhibit a behavior or meaning that the individual constituents do not."*[75] Since engineers/architects/developers do not design, code and maintain Applications, Services and Processes (ASP) in a vacuum, they need to embrace a "system of systems" mindset toward system interaction since there are legitimate cybersecurity and/or data protection concerns with untrustworthy dependencies. A system of systems is a *"set of systems and*

[73] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*
[74] *NIST SP 800-160 Vol 1 Rev 1*
[75] *NIST SP 800-160 Vol 1 Rev 1*

system elements interacting to provide a unique capability that none of the constituent systems can accomplish on their own."[76] A system of systems consists of several constituent systems plus any inter-system infrastructure, facilities and processes necessary to enable the constituent systems to integrate or interoperate.

This concept includes "interfacing systems" that have an interface for exchanging data or information, energy, or other resources. Interfacing systems have two specific subsets:

- Enabling Systems. These provide essential services required to create and sustain the system. Examples of enabling systems include:
  - Development environments;
  - Production systems, applications and services;
  - Training systems; and
  - Maintenance systems; and
- Interoperating Systems. These interact with systems to jointly perform a function during the utilization and sustainment stages of the system life cycle. Interoperating systems often form a system of systems.

[76] *NIST SP 800-160 Vol 1 Rev 1*

ANNEXES

ANNEX 1: CMMC LEVEL 1 REQUIREMENTS (INCLUDING ASSESSMENT OBJECTIVES)

Annex 1 to the CMMC Level 1 Assessment Guide:

- Contains the Set Theory Relationship Mapping (STRM) view of crosswalk mapping from CMMC Level 1 to SCF controls; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l1.xlsx

ANNEX 2: CMMC LEVEL 1 EVIDENCE REQUEST LIST (ERL)

Annex 3 to the CMMC Level 1 Assessment Guide:

- Contains a complete listing of CMMC Level 1-specific evidence artifacts; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l1.xlsx

ANNEX 3: SCF CAP RASCI

Annex 4 to the CMMC Level 1 Assessment Guide:

- Contains a RASCI matrix for 3PAAC Services; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l1.xlsx